Recueil de la jurisprudence

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

Affaire C-520/18

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,

[demande de décision préjudicielle formée par la Cour constitutionnelle (Belgique)]

« Renvoi préjudiciel – Traitement des données à caractère personnel et protection de la vie privée dans le secteur des communications électroniques – Directive 2002/58/CE – Champ d'application – Article 1er, paragraphe 3 – Article 15, paragraphe 1 – Article 4, paragraphe 2, TUE – Charte des droits fondamentaux de l'Union européenne – Articles 4, 6, 7, 8, 11 et article 52, paragraphe 1 – Obligation de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation – Effectivité des enquêtes pénales et autres objectifs d'intérêt général »

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

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

1 Langue originale : l'espagnol.

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

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

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

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

2. Ces arrêts (en particulier le deuxième) préoccupent les autorités de certains États membres, car, selon elles, ils ont pour effet de les priver d'un instrument qu'elles estiment nécessaire pour la sauvegarde de la sécurité nationale et la lutte contre la criminalité et le terrorisme. C'est pourquoi certains de ces États membres préconisent de renverser ou de nuancer cette jurisprudence.

3. Certaines juridictions des États membres ont mis en évidence cette même préoccupation dans quatre renvois préjudiciels[7], sur lesquels je présente ce jour mes conclusions.

4. Les quatre affaires soulèvent, avant tout, le problème de l'application de la directive 2002/58 aux activités liées à la sécurité nationale et à la lutte contre le terrorisme. Si cette directive devait s'appliquer dans ce contexte, il conviendrait alors de préciser dans quelle mesure les États membres peuvent restreindre les droits en matière de protection de la vie privée qu'elle garantit. Enfin, il y a lieu d'analyser dans quelle mesure les différentes réglementations nationales (du Royaume-Uni[8], belge[9] et française[10]) en la matière sont conformes au droit de l'Union, tel qu'interprété par la Cour.

5. Une fois l'arrêt Digital Rights Ireland e.a. connu, la Cour constitutionnelle (Belgique) a annulé la réglementation nationale qui avait partiellement transposé en droit national la directive 2006/24, déclarée invalide dans cet arrêt. Le législateur belge a ensuite adopté une nouvelle réglementation, dont la compatibilité avec le droit de l'Union a de nouveau été remise en cause à la suite de l'arrêt Tele2 Sverige et Watson e.a.

6. Une particularité du présent renvoi est qu'il soulève la question de savoir s'il est possible de maintenir provisoirement les effets d'une règle nationale dont l'annulation par les juridictions nationales s'impose en raison de son incompatibilité avec le droit de l'Union.

I. Le cadre juridique

A. Le droit de l'Union

7. Je renvoie à la section correspondante de mes conclusions dans les affaires jointes La Quadrature du Net e.a. (C-511/18 et C-512/18, EU:C:2020:6).

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

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

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

7 Outre la présente demande (affaire C-520/18, Ordre des barreaux francophones et germanophone e.a.), il s'agit des affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a., ainsi que de l'affaire C-623/17, Privacy International.

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

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

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

B. Le droit belge

8. L'article 4 de la loi relative à la collecte et à la conservation des données dans le secteur des communications électroniques [11], du 29 mai 2016, dispose que l'article 126 de la loi relative aux communications électroniques [12], du 13 juin 2005, est rédigé comme suit :

« § 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.

[...]

§ 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 [13] 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 [règles de sécurité des réseaux] 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 [...] 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

11 *Moniteur belge* du 18 juillet 2016, p. 44717, ci-après la « loi du 29 mai 2016 ».

12 *Moniteur belge* du 20 juin 2005, p. 28070, ci-après la « loi de 2005 ».

13 *Moniteur belge* du 18 décembre 1998, p. 40312, ci-après la « loi de 1998 ».

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 [...]. 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, 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.

§ 4. Pour la conservation des données visées au paragraphe 3, les fournisseurs et les opérateurs visés au paragraphe 1er, alinéa 1er :

1° garantissent que les données conservées sont de la même qualité et sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau ;

2° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites ;

3° garantissent que l'accès aux données conservées pour répondre aux demandes des autorités visées au paragraphe 2 n'est effectué que par un ou plusieurs membres de la Cellule de coordination visée à l'article 126/1, § 1er ;

4° conservent les données sur le territoire de l'Union européenne ;

5° mettent en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, illisibles et inutilisables par toute personne qui n'est pas autorisée à y avoir accès ;

6° détruisent les données conservées de tout support lorsqu'est expiré le délai de conservation applicable à ces données fixé au paragraphe 3, sans préjudice des articles 122 et 123 ;

7° assurent une traçabilité de l'exploitation des données conservées pour chaque demande d'obtention de ces données d'une autorité visée au paragraphe 2.

La traçabilité visée à l'alinéa 1er, 7°, s'effectue à l'aide d'un journal. L'Institut et la Commission pour la protection de la vie privée peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal. L'Institut et la Commission pour la protection de la vie privée concluent un protocole de collaboration concernant la prise de connaissance et le contrôle du contenu du journal.

§ 5. Le ministre et le ministre de la Justice font en sorte que des statistiques sur la conservation des données qui sont générées ou traitées dans le cadre de la fourniture de services ou réseaux de communications accessibles au public soient transmises annuellement à la Chambre des représentants.

Ces statistiques comprennent notamment :

1° les cas dans lesquels des données ont été transmises aux autorités compétentes conformément aux dispositions légales applicables ;

2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission ;

3° les cas dans lesquels des demandes de données n'ont pu être satisfaites.

Ces statistiques ne peuvent comprendre des données à caractère personnel.

[...] »

9. L'article 5 de la loi du 29 mai 2016 prévoit l'insertion d'un article 126/1 dans la loi de 2005, rédigé comme suit :

« § 1er. Au sein de chaque opérateur, et au sein de chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, est constituée une Cellule de coordination, chargée de fournir aux autorités belges légalement habilitées, à leur demande, des données conservées en vertu des articles 122, 123 et 126, les données d'identification de l'appelant en vertu de l'article 107, § 2, alinéa 1er, ou les données qui peuvent être requises en vertu des articles 46bis, 88bis et 90ter du Code d'instruction criminelle et des articles 18/7, 18/8, 18/16 et 18/17 de la [loi de 1998].

[...]

§ 2. Chaque opérateur et chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, établit une procédure interne permettant de répondre aux demandes d'accès des autorités aux données à caractère personnel concernant les utilisateurs. Il met, sur demande, à la disposition de l'Institut

des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse.

[...]

§ 3. Chaque fournisseur et chaque opérateur visés à l'article 126, § 1er, alinéa 1er, désigne un ou plusieurs préposés à la protection des données à caractère personnel, qui doit répondre aux conditions cumulatives énumérées au paragraphe 1er, alinéa 3.

[...]

Dans l'exercice de ses missions, le préposé à la protection des données à caractère personnel agit en toute indépendance, et a accès à toutes les données à caractère personnel transmises aux autorités ainsi qu'à tous les locaux pertinents du fournisseur ou de l'opérateur.

[...]

§ 4. Le Roi détermine, par arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut :

[...]

2° les exigences auxquelles la Cellule de coordination doit répondre, en prenant en compte la situation des opérateurs et fournisseurs recevant peu de demandes des autorités judiciaires, n'ayant pas d'établissement en Belgique ou opérant principalement de l'étranger ;

3° les informations à fournir à l'Institut et à la Commission pour la protection de la vie privée conformément aux paragraphes 1 et 3 ainsi que les autorités qui ont accès à ces informations ;

4° les autres règles régissant la collaboration des opérateurs et des fournisseurs visés à l'article 126, § 1er, alinéa 1er, avec les autorités belges ou avec certaines d'entre elles, pour la fourniture des données visées au paragraphe 1er, en ce compris, si nécessaire et par autorité concernée, la forme et le contenu de la demande.

[...] »

10. L'article 8 de la loi du 29 mai 2016 dispose que l'article 46bis, § 1er, du code d'instruction criminelle est modifié comme suit :

« § 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, en requérant au besoin le concours de l'opérateur d'un réseau de communication électronique ou d'un fournisseur d'un service de communication électronique ou d'un service de police désigné par le Roi, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d'un accès aux fichiers des clients de l'opérateur ou du fournisseur de service à :

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilisé ;

2° l'identification des services de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête.

En cas d'extrême urgence, chaque officier de police judiciaire peut, avec l'accord oral et préalable du procureur du Roi, et par une décision motivée et écrite requérir ces données. L'officier de police judiciaire communique cette décision motivée et écrite ainsi que les informations recueillies dans les vingt-quatre heures au procureur du Roi et motive par ailleurs l'extrême urgence.

Pour des infractions qui ne sont pas de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, le procureur du Roi, ou, en cas d'extrême urgence, l'officier de police judiciaire, ne peuvent requérir les données visées à l'alinéa 1er que pour une période de six mois préalable à sa décision.

§ 2. Chaque opérateur d'un réseau de communication électronique et chaque fournisseur d'un service de communication électronique qui est requis de communiquer les données visées au paragraphe premier, donne au procureur du Roi ou à l'officier de police judiciaire les données qui ont été demandées dans un délai à fixer par le Roi [...]

[...]

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Le refus de communiquer les données est puni d'une amende de vingt-six euros à dix mille euros. »

11. En vertu de l'article 9 de la loi du 29 mai 2016, l'article 88bis du code d'instruction criminelle est libellé comme suit :

« § 1er. S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut procéder ou faire procéder, en requérant au besoin, directement ou par l'intermédiaire d'un service de police désigné par le Roi, le concours technique de l'opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique :

1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées ;

2° à la localisation de l'origine ou de la destination de communications électroniques.

Dans les cas visés à l'alinéa 1er, pour chaque moyen de communication électronique dont les données d'appel sont repérées ou dont l'origine ou la destination de la télécommunication est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un procès-verbal.

Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête, dans une ordonnance motivée.

Il précise également la durée durant laquelle [la mesure] pourra s'appliquer pour le futur, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement et, le cas échéant, la période pour le passé sur laquelle l'ordonnance s'étend conformément au paragraphe 2.

[...]

§ 2. Pour ce qui concerne l'application de la mesure visée au paragraphe 1er, alinéa 1er, aux données de trafic ou de localisation conservées sur la base de l'article 126 de la loi [de 2005], les dispositions suivantes s'appliquent :

– pour une infraction visée au livre II, titre Iter, du Code pénal, le juge d'instruction peut dans son ordonnance requérir les données pour une période de douze mois préalable à l'ordonnance ;

– pour une autre infraction visée à l'article 90ter, §§ 2 à 4, qui n'est pas visée au premier tiret ou pour une infraction qui est commise dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal, ou pour une infraction qui est de nature à entraîner un emprisonnement correctionnel principal de cinq ans ou une peine plus lourde, le juge d'instruction peut dans son ordonnance requérir les données pour une période de neuf mois préalable à l'ordonnance ;

– pour les autres infractions, le juge d'instruction ne peut requérir les données que pour une période de six mois préalable à l'ordonnance.

§ 3. La mesure ne peut porter sur les moyens de communication électronique d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une infraction visée au paragraphe 1er ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une infraction visée au paragraphe 1er, utilisent ses moyens de communication électronique.

La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par le juge d'instruction des éléments qu'il estime relever du secret professionnel. Ces éléments ne sont pas consignés au procès-verbal.

§ 4. [...]

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

[...] »

12. Conformément à l'article 12 de la loi du 29 mai 2016, l'article 13 de la loi de 1998 est rédigé comme suit :

« [Les services de renseignement et de sécurité] peuvent rechercher, collecter, recevoir et traiter des informations et des données à caractère personnel qui peuvent être utiles à l'exécution de leurs missions et tenir à jour une documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de leurs missions.

Les renseignements contenus dans la documentation doivent présenter un lien avec la finalité du fichier et se limiter aux exigences qui en découlent.

Les services de renseignement et de sécurité veillent à la sécurité des données ayant trait à leurs sources et à celles des informations et des données à caractère personnel fournies par ces sources.

Les agents des services de renseignement et de sécurité ont accès aux informations, renseignements et données à caractère personnel recueillis et traités par leur service, pour autant que ceux-ci soient utiles dans l'exercice de leur fonction ou de leur mission. »

13. L'article 14 de la loi du 29 mai 2016 donne un nouveau libellé à l'article 18/3 de la loi de 1998, qui dispose désormais :

« § 1. Les méthodes spécifiques de recueil de données visées à l'article 18/2, § 1er, peuvent être mises en œuvre compte tenu de la menace potentielle visée à l'article 18/1, si les méthodes ordinaires de recueil de données sont jugées insuffisantes pour permettre de récolter les informations nécessaires à l'aboutissement d'une mission de renseignement. La méthode spécifique doit être choisie en fonction du degré de gravité de la menace potentielle pour laquelle elle est mise en œuvre.

La méthode spécifique ne peut être mise en œuvre qu'après décision écrite et motivée du dirigeant du service et après notification de cette décision à la commission.

§ 2. La décision du dirigeant du service mentionne :

1° la nature de la méthode spécifique ;

2° selon le cas, les personnes physiques ou morales, les associations ou les groupements, les objets, les lieux, les événements ou les informations soumis à la méthode spécifique ;

3° la menace potentielle qui justifie la méthode spécifique ;

4° les circonstances de fait qui justifient la méthode spécifique, la motivation en matière de subsidiarité et de proportionnalité, en ce compris le lien entre le 2° et le 3° ;

5° la période pendant laquelle la méthode spécifique peut être appliquée, à compter de la notification de la décision à la Commission ;

[...]

9° le cas échéant, les indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle ;

10° dans le cas où il est fait application de l'article 18/8, la motivation de la durée de la période à laquelle a trait la collecte de données ;

[...]

§ 8. Le dirigeant du service met fin à la méthode spécifique lorsque la menace potentielle qui la justifie a disparu, lorsque la méthode n'est plus utile pour la finalité pour laquelle elle avait été mise en œuvre, ou quand il a constaté une illégalité. Il informe dans les plus brefs délais la Commission de sa décision. »

14. L'article 18/8 de la loi de 1998 est désormais libellé comme suit :

« § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, au besoin en requérant à cette fin le concours technique de l'opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique, procéder ou faire procéder :

1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées ;

2° à la localisation de l'origine ou de la destination de communications électroniques.

[...]

§ 2. Pour ce qui concerne l'application de la méthode visée au paragraphe 1er aux données conservées sur la base de l'article 126 de la loi [de 2005], les dispositions suivantes s'appliquent :

1° pour une menace potentielle qui se rapporte à une activité qui peut être liée aux organisations criminelles ou aux organisations sectaires nuisibles, le dirigeant du service ne peut dans sa décision requérir les données que pour une période de six mois préalable à la décision ;

2° pour une menace potentielle autre que celles visées sous le 1° et le 3°, le dirigeant du service peut dans sa décision requérir les données pour une période de neuf mois préalable à la décision ;

3° pour une menace potentielle qui se rapporte à une activité qui peut être liée au terrorisme ou à l'extrémisme, le dirigeant du service peut dans sa décision requérir les données pour une période de douze mois préalable à la décision [...] »

II. Les faits de la procédure au principal et les questions préjudicielles

15. Dans son arrêt du 11 juin 2015[14], la Cour constitutionnelle a annulé la nouvelle version de l'article 126 de la loi de 2005, pour les raisons qui avaient conduit la Cour à déclarer la directive 2006/24 invalide dans l'arrêt Digital Rights Ireland e.a.

[14] Arrêt nº 84/2015, *Moniteur belge* du 11 août 2015.

16. Au vu de cette annulation, le législateur national a adopté (avant le prononcé de l'arrêt Tele2 Sverige et Watson e.a.) la loi du 29 mai 2016.

17. VZ et autres, l'Ordre des barreaux francophones et germanophone (ci-après l'« Ordre des barreaux »), l'ASBL « Liga voor Mensenrechten » (ci-après la « LMR »), l'ASBL « Ligue des Droits de l'Homme » (ci-après la « LDH ») et l'ASBL « Académie Fiscale » (ci-après l'« Académie Fiscale ») ont saisi la juridiction de renvoi de plusieurs recours en annulation fondés sur l'inconstitutionnalité de ladite loi en soutenant, en substance, qu'elle dépassait les limites du strict nécessaire et n'offrait pas des garanties suffisantes de protection.

18. Dans ce contexte, la Cour constitutionnelle a posé les questions préjudicielles suivantes à la Cour :

« 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 l'article 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 communication électronique, ou la réalisation d'un autre objectif identifié par l'article 23, paragraphe 1, du règlement (UE) 2016/679 [du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO 2016, L 119, p. 1)], 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 l'article 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 8 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 attaquée 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 ? »

III. La procédure devant la Cour

19. Le renvoi préjudiciel a été enregistré au greffe de la Cour le 2 août 2018.

20. VZ et autres, l'Académie Fiscale, la LMR, la LDH, l'Ordre des barreaux, la Fondation pour Enfants Disparus et Sexuellement Exploités (Child Focus), les gouvernements belge, tchèque, danois, allemand, estonien, irlandais, espagnol, français, chypriote, hongrois, néerlandais, polonais, suédois et du Royaume-Uni ainsi que la Commission européenne ont présenté des observations écrites.

21. Les parties aux quatre renvois préjudiciels, les gouvernements susmentionnés et celui du Royaume de Norvège ainsi que la Commission et le Contrôleur européen de la protection des données (CEPD) ont comparu lors de l'audience de plaidoiries qui s'est tenue le 9 septembre 2019, concernant également les affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a., ainsi que l'affaire C-623/17, Privacy International.

IV. Analyse

22. La première question du présent renvoi coïncide, en substance, avec celles des affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a. Elle diffère cependant de ces dernières quant aux objectifs poursuivis par la réglementation nationale, qui vise non seulement la lutte contre le terrorisme et les formes les plus graves de criminalité ou la garantie de la sécurité nationale, mais aussi « la défense du territoire et de la sécurité publique, la recherche, la détection et la poursuite d'autres faits que ceux de criminalité grave » et, de manière générale, tous ceux visés à l'article 23, paragraphe 1, du règlement 2016/679.

23. La deuxième question est liée à la première, mais la complète en ce qu'elle demande si les obligations positives incombant à l'autorité publique en matière d'enquête et de répression des abus sexuels à l'égard de mineurs justifieraient les mesures litigieuses.

24. La troisième question est posée dans l'hypothèse où la réglementation nationale serait incompatible avec le droit de l'Union. La juridiction de renvoi souhaite savoir si, dans cette hypothèse, elle pourrait maintenir provisoirement les effets de la loi du 29 mai 2016.

25. Je traiterai ces questions en analysant, en premier lieu, l'applicabilité de la directive 2002/58, en renvoyant sur ce point à mes conclusions dans les autres renvois préjudiciels susvisés. En deuxième lieu, je présenterai les grandes lignes de la jurisprudence de la Cour en la matière et ses évolutions possibles. J'aborderai, en troisième lieu, la réponse à donner à chacune de ces questions préjudicielles.

A. L'applicabilité de la directive 2002/58

26. Comme dans les trois autres renvois préjudiciels, le présent renvoi met en doute l'applicabilité de la directive 2002/58. Les thèses des États membres à ce sujet étant identiques, je renvoie à mes conclusions dans les affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a.[15], à cet égard.

[15] Points 40 et suiv.

B. La jurisprudence de la Cour relative à la conservation des données à caractère personnel et à l'accès des autorités publiques à ces données dans le cadre de la directive 2002/58

1. Le principe de confidentialité des communications et des données connexes

27. Les dispositions de la directive 2002/58 « précisent et complètent » la directive 95/46/CE [16] afin d'atteindre un niveau élevé de protection des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques [17].

28. L'article 5, paragraphe 1, de la directive 2002/58 dispose que les États membres doivent garantir, dans leur 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.

29. La confidentialité des communications implique, entre autres (article 5, paragraphe 1, deuxième phrase, de la directive 2002/58), l'interdiction faite à toute autre personne que les utilisateurs de stocker, sans leur consentement, les données relatives au trafic afférentes aux communications électroniques. Font l'objet d'exceptions « les personnes légalement autorisées [...] et le stockage technique nécessaire à l'acheminement d'une communication » [18].

30. Les articles 5 et 6 ainsi que l'article 9, paragraphe 1, de la directive 2002/58 visent à préserver la confidentialité des communications et des données y afférentes et à minimiser le risque d'abus. Leur portée doit être appréciée à la lumière du considérant 30 de cette directive, selon lequel « [l]es 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 » [19].

31. Quant à ces données, on peut distinguer :

– les données relatives au *trafic*, dont le traitement et le stockage ne sont autorisés que dans la mesure et pour la durée indispensables à la facturation et à la commercialisation des services et à la fourniture de services à valeur ajoutée (article 6 de la directive 2002/58). Une fois cette durée expirée, les données traitées et stockées doivent être effacées ou rendues anonymes [20] ; et

– les données de *localisation* autres que les données relatives au trafic, qui ne peuvent être traitées que sous certaines conditions et après les avoir rendues anonymes ou avoir obtenu le consentement des utilisateurs ou des abonnés (article 9, paragraphe 1, de la directive 2002/58) [21].

16 Directive du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31). Voir article 1er, paragraphe 2, de la directive 2002/58. La directive 95/46 a été abrogée avec effet au 25 mai 2018 par le règlement 2016/679. Par conséquent, dans la mesure où la directive 2002/58 fait référence à la directive 95/46 ou n'établit pas de règles elle-même, il est indispensable de tenir compte des dispositions dudit règlement (voir article 94, paragraphes 1 et 2, du règlement 2016/679).

17 Voir arrêt Tele2 Sverige et Watson e.a. (points 82 et 83).

18 Arrêt Tele2 Sverige et Watson e.a. (point 85 et jurisprudence citée).

19 Arrêt Tele2 Sverige et Watson e.a. (point 87). Mise en italique par mes soins.

20 Arrêt Tele2 Sverige et Watson e.a. (point 86 et jurisprudence citée).

21 Arrêt Tele2 Sverige et Watson e.a. (point 86 in fine).

2. La clause de limitation prévue à l'article 15, paragraphe 1, de la directive 2002/58

32. L'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'« 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 cette directive.

33. Toute limitation doit constituer « 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] ».

34. Cette énumération d'objectifs revêt un caractère exhaustif[22] : à titre d'exemple (« entre autres »), les « mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe » sont permises.

35. En tout état de cause, « [t]outes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne ». Dès lors, l'article 15, paragraphe 1, de la directive 2002/58 doit être interprété à la lumière des droits fondamentaux garantis par la Charte[23].

36. Parmi les droits reconnus dans la Charte, la Cour a mentionné, pour ce qui nous occupe, le droit au respect de la vie privée (article 7), le droit à la protection des données à caractère personnel (article 8) et le droit à la liberté d'expression (article 11)[24].

37. La Cour a en outre souligné, comme critère orientant son interprétation de l'article 15, paragraphe 1, de la directive 2002/58, que les limitations à l'obligation de garantir la confidentialité des communications et des données relatives au trafic y afférentes doivent être interprétées strictement.

38. Elle a concrètement exclu la possibilité « que la dérogation à cette obligation de principe et, en particulier, à l'interdiction de stocker ces données, prévue à l'article 5 de cette directive, devienne la règle, sauf à vider largement cette dernière disposition de sa portée »[25].

39. Cette double observation me semble déterminante pour comprendre les raisons pour lesquelles la Cour a estimé que la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation afférentes aux communications électroniques était incompatible avec la directive 2002/58.

22 Arrêt Tele2 Sverige et Watson e.a. (point 90).

23 Arrêt Tele2 Sverige et Watson e.a. (point 91 et jurisprudence citée).

24 Arrêt Tele2 Sverige et Watson e.a. (point 93 et jurisprudence citée).

25 Arrêt Tele2 Sverige et Watson e.a. (point 89).

40. Cette constatation de la Cour n'a fait que mettre en œuvre « rigoureusement » [26] le critère de proportionnalité qu'elle avait déjà utilisé auparavant [27] : « la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige 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 » [28].

3. La proportionnalité dans la conservation des données

a) Le caractère disproportionné de la conservation généralisée et indifférenciée

41. La Cour reconnaît que la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et que son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête. Elle ajoute que, « [t]outefois, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte » [29].

42. Afin de déterminer si une telle mesure se limitait au strict nécessaire, la Cour a souligné, avant toute chose, la gravité particulière de l'ingérence qu'elle causait dans les droits fondamentaux consacrés par les articles 7 et 8 de la Charte [30]. Cette gravité particulière résultait justement du fait que la législation nationale prévoyait « une conservation généralisée et indifférenciée de *l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique*, et [obligeait] les fournisseurs de services de communications électroniques à conserver ces données *de manière systématique et continue, et ce sans aucune exception* » [31].

43. L'ingérence que cette mesure comportait dans la vie des justiciables est reflétée dans ces appréciations de la Cour sur les effets de la conservation des données.

Ces données [32] :

– « permettent de retrouver et d'identifier la source d'une communication et la destination de celle-ci, de déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que de localiser le matériel de communication mobile » [33] ;

– « permettent, en particulier, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent

26 L'usage de cet adverbe au point 95 de l'arrêt Tele2 Sverige et Watson e.a. provient du considérant 11 de la directive 2002/58.

27 Arrêt Digital Rights Ireland e.a., point 48 : « compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict ».

28 Arrêt Tele2 Sverige et Watson e.a. (point 96 et jurisprudence citée).

29 Arrêt Digital Rights Ireland e.a. (point 51). Voir, en ce sens, arrêt Tele2 Sverige et Watson e.a. (point 103).

30 Arrêts Digital Rights Ireland e.a. (point 65), ainsi que Tele2 Sverige et Watson e.a. (point 100).

31 Arrêt Tele2 Sverige et Watson e.a. (point 97). Mise en italique par mes soins.

32 Au nombre desquelles figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet.

33 Arrêt Tele2 Sverige et Watson e.a. (point 98).

de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée »[34] ;

– « sont susceptibles de 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 »[35] ;

– « 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 »[36].

44. L'ingérence peut en outre susciter « dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante », car « la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés »[37].

45. Eu égard à la gravité de l'ingérence, seule la lutte contre la criminalité grave serait susceptible de justifier une mesure de conservation des données présentant ces caractéristiques[38]. Celle-ci ne saurait toutefois devenir la règle générale, car « le système mis en place par la directive 2002/58 exige que cette conservation des données soit l'exception »[39].

46. De plus, deux caractéristiques résultaient du fait que la mesure en cause n'établissait « aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi »[40] et « ne requ[érait] aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique »[41] :

– d'une part, la mesure concernait « 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. [...] En outre, elle ne prévo[yait] aucune exception, de telle sorte qu'elle s'appliqu[ait] même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel »[42] ;

– d'autre part, elle n'était « 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 »[43].

34 Arrêt Tele2 Sverige et Watson e.a. (point 98).
35 Arrêt Tele2 Sverige et Watson e.a. (point 99).
36 Arrêt Tele2 Sverige et Watson e.a. (point 99 in fine).
37 Arrêt Tele2 Sverige et Watson e.a. (point 100).
38 Arrêt Tele2 Sverige et Watson e.a. (point 102).
39 Arrêt Tele2 Sverige et Watson e.a. (point 104).
40 Arrêt Tele2 Sverige et Watson e.a. (point 105).
41 Arrêt Tele2 Sverige et Watson e.a. (point 106).
42 Arrêt Tele2 Sverige et Watson e.a. (point 105).
43 Arrêt Tele2 Sverige et Watson e.a. (point 106).

47. Dans ces conditions, la législation nationale analysée excédait les limites du strict nécessaire. Elle ne pouvait donc être considérée comme étant justifiée dans une société démocratique, comme 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 [44].

b) La viabilité d'une conservation ciblée des données

48. La Cour a admis la conformité au droit de l'Union d'une législation nationale « permettant, à titre préventif, la *conservation ciblée* des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave » [45].

49. La viabilité de cette conservation ciblée est subordonnée à la condition qu'elle « 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 ».

50. Les orientations fournies dans l'arrêt Tele2 Sverige et Watson e.a. pour savoir quand ces conditions sont remplies ne sont pas exhaustives (et ne pouvaient peut-être pas l'être) et sont formulées en termes plutôt généraux. Pour les respecter, les États membres doivent :

– édicter des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données [46] ;

– fixer des « critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi » [47] ; et

– se fonder « sur des éléments objectifs permettant de viser un public dont les données 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 » [48].

51. Concernant ces éléments objectifs, la Cour mentionne, à titre d'exemple, la possibilité d'utiliser un critère géographique pour délimiter le public et les situations potentiellement concernés. L'invocation de ce critère, auquel certains États membres ont fait référence en des termes critiques, ne vise pas, selon moi, à limiter à lui seul l'éventail des facteurs de ciblage admissibles.

44 Arrêt Tele2 Sverige et Watson e.a. (point 107).

45 Arrêt Tele2 Sverige et Watson e.a. (point 108). Mise en italique par mes soins.

46 Arrêt Tele2 Sverige et Watson e.a. (point 109). En particulier, ils doivent indiquer « en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise, garantissant ainsi qu'une telle mesure soit limitée au strict nécessaire ».

47 Arrêt Tele2 Sverige et Watson e.a. (point 110).

48 Arrêt Tele2 Sverige et Watson e.a. (point 111).

4. La proportionnalité de l'accès aux données

a) L'arrêt Tele2 Sverige et Watson e.a.

52. La Cour envisage l'*accès* des autorités nationales aux données indépendamment de la portée de l'obligation de *conservation* imposée aux fournisseurs de services de communications électroniques et, en particulier, du caractère généralisé ou ciblé de la conservation de ces données [49].

53. En effet, bien que la logique de la conservation soit de faciliter l'accès ultérieur aux données, tant la conservation que l'accès peuvent entraîner des violations distinctes des droits fondamentaux protégés par la Charte. Cette différenciation n'implique cependant pas que certaines considérations relatives à la conservation ne valent pas également pour l'accès aux données conservées.

54. En ce sens, l'accès :

– « doit répondre effectivement et strictement à l'un [des] objectifs » figurant à l'article 15, paragraphe 1, première phrase, de la directive 2002/58. De plus, la gravité de l'ingérence doit concorder avec l'objectif poursuivi. Si l'ingérence est qualifiée de grave, elle ne peut être justifiée que par la lutte contre la criminalité grave [50] ;

– peut uniquement être autorisé dans les limites du strict nécessaire [51]. Qui plus est, les mesures législatives doivent prévoir « des règles claires et précises indiquant en quelles circonstances et sous quelles conditions les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données. De même, une mesure de cette nature doit être légalement contraignante en droit interne » [52] ;

– plus précisément, les réglementations nationales doivent fixer « les conditions matérielles et procédurales régissant l'accès des autorités nationales compétentes aux données conservées » [53].

55. On peut déduire de ce qui précède qu'« un accès général à toutes les données conservées, indépendamment d'un quelconque lien, à tout le moins indirect, avec le but poursuivi, ne saurait être considéré comme limité au strict nécessaire » [54].

56. La Cour relève que « la réglementation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données des abonnés ou des utilisateurs inscrits » [55]. À cet égard, « un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'*aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction* » [56].

49 Arrêt Tele2 Sverige et Watson e.a. (point 113).

50 Arrêt Tele2 Sverige et Watson e.a. (point 115).

51 Arrêt Tele2 Sverige et Watson e.a. (point 116).

52 Arrêt Tele2 Sverige et Watson e.a. (point 117).

53 Arrêt Tele2 Sverige et Watson e.a. (point 118).

54 Arrêt Tele2 Sverige et Watson e.a. (point 119).

55 Arrêt Tele2 Sverige et Watson e.a. (point 119).

56 Arrêt Tele2 Sverige et Watson e.a. (point 119). Mise en italique par mes soins.

57. En d'autres termes, les règles nationales accordant aux autorités nationales compétentes l'accès aux données conservées doivent avoir une portée suffisamment limitée. Il doit exister un lien entre les personnes concernées et l'objectif poursuivi, de sorte que l'accès ne couvre pas un nombre significatif de personnes, voire toutes les personnes, tous les moyens de communication électronique et toutes les données stockées.

58. Ces règles peuvent néanmoins être tempérées dans certaines circonstances. La Cour évoque des « situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme ». Dans de telles situations, « l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités » [57].

59. Cette précision donnée par la Cour permet aux États membres de mettre en place un régime spécifique d'accès aux données plus étendu, lorsque cela est exceptionnellement nécessaire pour lutter contre les menaces pesant sur les intérêts primordiaux de l'État (la sécurité nationale, la défense et la sécurité publique) [58], de telle sorte qu'il inclue même les personnes ayant un lien seulement indirect avec ces risques.

60. L'accès des autorités nationales aux données stockées, de quelque nature qu'elles soient, doit être soumis à trois conditions :

– il doit être soumis « en principe, sauf cas d'urgence dûment justifiés, [...] à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante ». La décision de cette juridiction ou entité doit être adoptée « à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales » [59] ;

– « les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités » [60] ;

– les États membres doivent adopter des règles relatives à la sécurité et à la protection des données détenues par les fournisseurs de services de communications électroniques afin de prévenir toute utilisation abusive et tout accès illicite aux données [61].

b) L'arrêt Ministerio Fiscal

61. Dans cette affaire, il était demandé si une réglementation nationale prévoyant l'accès des autorités compétentes aux données relatives à l'identité civile des titulaires de certaines cartes SIM était compatible avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte.

57 Arrêt Tele2 Sverige et Watson e.a. (point 119).

58 Outre les activités terroristes, d'autres éventualités, telles qu'une attaque informatique de grande envergure contre des infrastructures critiques de l'État ou une menace liée à la prolifération nucléaire, pourraient justifier ce caractère exceptionnel.

59 Arrêt Tele2 Sverige et Watson e.a. (point 120).

60 Arrêt Tele2 Sverige et Watson e.a. (point 121).

61 Arrêt Tele2 Sverige et Watson e.a. (point 122).

62. La Cour a jugé que l'article 15, paragraphe 1, première phrase, de la directive 2002/58 ne limite pas l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales à la lutte contre les seules infractions graves, mais vise les « infractions pénales » en général [62].

63. J'ajouterai que, pour justifier l'accès aux données par les autorités nationales compétentes, il doit exister une correspondance entre la gravité de l'ingérence et celle des infractions en question. Par conséquent :

– « une ingérence grave ne peut être justifiée [...] que par un objectif de lutte contre la criminalité devant également être qualifiée de "grave" » [63] ;

– en revanche, « lorsque l'ingérence que comporte un tel accès n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d'"infractions pénales" en général » [64].

64. Sur la base de cette prémisse, à la différence de l'arrêt Tele2 Sverige et Watson e.a., la Cour n'a pas qualifié de « grave » l'atteinte aux droits protégés par les articles 7 et 8 de la Charte, car la demande d'accès avait « pour seul objet d'identifier les titulaires des cartes SIM activées, pendant une période de douze jours, avec le code IMEI du téléphone mobile volé » [65].

65. Afin de souligner le caractère moins grave de l'ingérence, elle explique que « les données visées par la demande d'accès en cause au principal permettent uniquement de mettre en relation, pendant une période déterminée, la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM. Sans un recoupement avec les données afférentes aux communications effectuées avec lesdites cartes SIM et les données de localisation, ces données ne permettent de connaître ni la date, l'heure, la durée et les destinataires des communications effectuées avec la ou les cartes SIM en cause, ni les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée. Lesdites données ne permettent donc pas de tirer de conclusions précises concernant la vie privée des personnes dont les données sont concernées » [66].

66. Dans l'affaire tranchée par l'arrêt Ministerio Fiscal, il ne s'agissait pas de savoir si les données à caractère personnel faisant l'objet d'un accès avaient été conservées par les fournisseurs de services de communications électroniques dans le respect des conditions visées à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte [67]. La question de savoir s'il était satisfait ou non aux autres conditions d'accès découlant de cet article n'a pas non plus été abordée.

62 Arrêt Ministerio Fiscal (point 53).

63 Arrêt Ministerio Fiscal (point 56).

64 Arrêt Ministerio Fiscal (point 57).

65 Arrêt Ministerio Fiscal (point 59). Il s'agissait de l'accès aux « numéros de téléphone correspondant à ces cartes SIM ainsi qu'aux données relatives à l'identité civile des titulaires desdites cartes, telles que leurs nom, prénom et, le cas échéant, adresse. En revanche, ces données ne port[ai]ent pas, comme l'ont confirmé tant le gouvernement espagnol que le ministère public lors de l'audience, sur les communications effectuées avec le téléphone mobile volé ni sur la localisation de celui-ci ».

66 Arrêt Ministerio Fiscal (point 60).

67 Arrêt Ministerio Fiscal (point 49).

67. Il s'ensuit que la lecture de l'arrêt Ministerio Fiscal ne permet de déduire aucun changement dans la jurisprudence de la Cour concernant l'incompatibilité avec le droit de l'Union d'un régime national autorisant la conservation généralisée et indifférenciée des données, au sens de l'arrêt Tele2 Sverige et Watson e.a.

68. J'estime toutefois que, en reconnaissant la validité du régime d'accès limité à certaines données à caractère personnel (celles relatives à l'identité civile des titulaires de cartes SIM), la Cour accepte implicitement la conservation de ces mêmes données par les fournisseurs de services.

C. Les principales critiques à l'égard de la jurisprudence de la Cour

69. Tant la juridiction de renvoi que la majorité des États membres qui ont présenté des observations invitent la Cour à clarifier, nuancer, voire reconsidérer plusieurs aspects de sa jurisprudence dans ce domaine, qui est la cible de leurs critiques.

70. La plupart de ces critiques, voilées ou frontales, ont déjà été exprimées à l'occasion de l'arrêt Digital Rights Ireland e.a. et ont été rejetées dans l'arrêt Tele2 Sverige et Watson e.a. Elles ressurgissent désormais pour souligner, en somme, que des règles rigoureuses en matière d'accès aux données détenues par les fournisseurs de services de communications électroniques pouvant compenser, dans une certaine mesure, la gravité de l'ingérence causée par la conservation généralisée et indifférenciée de ces mêmes données suffiraient.

71. Plusieurs de ces critiques mettent également en exergue la nécessité de mesures réellement efficaces dans la lutte contre les menaces graves envers la sécurité et contre la criminalité en général, et il est demandé à la Cour de tenir compte du droit à la sûreté (article 6 de la Charte), ainsi que de la marge d'appréciation des États membres pour sauvegarder la sécurité nationale. Dans certains cas, il est ajouté que la Cour n'a pas pris en compte le caractère préventif de l'intervention des services de sécurité et de renseignement.

D. Mon appréciation de ces critiques et des nuances qui pourraient être apportées à la jurisprudence de la Cour

72. À mon sens, la Cour devrait maintenir la position de principe à laquelle elle est parvenue dans ses précédents arrêts : une obligation généralisée et indifférenciée de conserver l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits porte une atteinte disproportionnée aux droits fondamentaux protégés par les articles 7, 8 et 11 de la Charte.

73. A contrario, une législation nationale prévoyant des restrictions appropriées à la conservation de certaines de ces données, générées dans le cadre de la fourniture de services de communications électroniques, pourrait être compatible avec le droit de l'Union. La clé réside donc dans la *conservation limitée* de ces données.

74. Pour les motifs que j'exposerai ci-après, cette conservation limitée ne devrait pas être circonscrite à celle visant une zone géographique ou une catégorie de personnes déterminées : les débats sur ces critères de conservation révèlent qu'ils pourraient être irréalisables ou inopérants aux fins recherchées, voire devenir source de discrimination.

75. D'emblée, je ne partage pas l'argument critique en faveur du binôme consistant dans la « conservation plus étendue en échange d'un accès plus restreint ». Le raisonnement de la Cour, auquel je souscris, est que la conservation et l'accès aux données constituent deux types d'ingérence distincts. Bien que la conservation des données ait un sens en vue d'un éventuel accès ultérieur par les autorités compétentes, chacune de ces ingérences devrait être justifiée séparément, au moyen d'une appréciation spécifique au regard de l'objectif poursuivi.

76. Ainsi, un système national prévoyant la conservation généralisée et indifférenciée de données ne peut être justifié au motif que, parallèlement, des règles soumettent l'accès à ces données à des exigences matérielles et procédurales strictes.

77. Il doit donc exister des règles spécifiques en matière de conservation des données qui soumettent celle-ci à certaines conditions pour qu'elle n'ait pas un caractère généralisé et indifférencié. C'est la seule manière de garantir sa compatibilité avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8, 11 et de l'article 52, paragraphe 1, de la Charte.

78. Telle est d'ailleurs l'approche adoptée par les groupes de travail réunis au sein du Conseil de l'Union européenne pour définir des règles de conservation et d'accès compatibles avec la jurisprudence de la Cour, en examinant en parallèle les deux types d'ingérence [68].

79. L'application de limites à chacun de ces deux types d'ingérence permettra d'apprécier si leur éventuel effet cumulatif, combiné avec des garanties solides, est de nature à atténuer l'incidence de la conservation des données sur les droits fondamentaux protégés par les articles 7, 8 et 11 de la Charte, tout en assurant l'efficacité des enquêtes.

80. Pour protéger ces droits, le système doit :

– prévoir une conservation des données qui comporte certaines limites et différences en fonction de l'objectif poursuivi ;

– prévoir l'accès à ces données uniquement dans la mesure strictement nécessaire à la finalité poursuivie et sous le contrôle d'une juridiction ou d'une autorité administrative indépendante.

81. La justification de l'obligation pour les fournisseurs de services de communications électroniques de conserver certaines données, et ce pas uniquement pour la gestion de leurs obligations contractuelles envers les utilisateurs, augmente parallèlement à l'évolution technologique. En admettant que cette conservation est utile pour prévenir et combattre la criminalité (ce qui est difficilement réfutable [69]), il ne semblerait pas logique de la circonscrire à la simple exploitation des données que les opérateurs conservent pour l'exercice de leurs activités commerciales et uniquement pour la durée nécessaire à celles-ci.

82. Une fois reconnue l'utilité d'une obligation de conservation des données pour sauvegarder la sécurité nationale et lutter contre la criminalité, outre celle que les opérateurs peuvent réaliser pour leurs besoins techniques et commerciaux, il est essentiel de définir les contours de cette obligation.

68 Depuis 2017, les États membres participent à un groupe de travail dont l'objectif est de mettre leur législation en conformité avec les critères fixés par la jurisprudence de la Cour en la matière [Groupe Échange d'informations et protection des données (DAPIX)].

69 En tout état de cause, la détermination des techniques d'investigation et l'appréciation de leur efficacité relèvent de la marge d'appréciation des États membres.

83. Chaque régime de conservation doit être strictement adapté à la finalité poursuivie, de sorte qu'il ne puisse se transformer en une conservation indifférenciée[70]. Il doit en outre exclure la possibilité que la somme de ces données offre un *portrait* de la personne concernée (c'est-à-dire de ses activités habituelles et de ses relations sociales) proche de celui qui serait obtenu en connaissant le contenu des communications ou semblable.

84. Afin de dissiper certains malentendus et certaines incompréhensions, il importe de tenir compte de ce que la Cour n'a *pas jugé* dans ses arrêts Digital Rights Ireland e.a. et Tele2 Sverige et Watson e.a. Ces arrêts ne condamnent pas l'existence, en tant que telle, d'un régime de conservation des données en tant qu'instrument utile de lutte contre la criminalité. Au contraire, la légitimité de l'objectif de prévention et de répression des actes criminels a été reconnue, ainsi que l'utilité d'un régime de conservation des données à cette fin.

85. Ce que, j'insiste sur ce point, la Cour a alors rejeté, et ce catégoriquement, c'est la possibilité que, en invoquant cet objectif, l'Union ou ses États membres imposent la conservation indifférenciée de *toutes* les données produites dans le cadre de la fourniture de services de communications électroniques et l'accès général à ces données.

86. Il est donc nécessaire de trouver des moyens de conservation des données qui préservent celle-ci des qualifications (« généralisée et indifférenciée ») incompatibles avec la protection requise par les articles 7, 8 et 11 de la Charte.

87. L'une de ces modalités serait la conservation *ciblée* des données, relatives soit à un public spécifique (en théorie, celui présentant certains liens, plus ou moins directs, avec les menaces les plus graves), soit à une zone géographique déterminée.

88. Cette approche pose toutefois certaines difficultés :

– l'identification d'un groupe d'agresseurs potentiels serait probablement insuffisante si ces derniers utilisaient des techniques d'anonymisation ou une fausse identité. Le choix de ces groupes pourrait également conduire à une suspicion générale à l'égard de certains segments de la population et être qualifié de discriminatoire, selon l'algorithme utilisé ;

– la sélection par critères géographiques (qui, pour être efficace, nécessiterait de cibler des zones qui ne soient pas trop étroites) pose les mêmes problèmes et d'autres encore, comme l'a indiqué le CEPD lors de l'audience, dans la mesure où elle pourrait stigmatiser certaines zones.

89. En outre, il peut y avoir une certaine contradiction entre le caractère préventif de la conservation visant un public spécifique ou une zone géographique et le fait que les auteurs des crimes ne sont pas connus à l'avance, pas plus que le lieu et la date de la commission de ces crimes.

90. En tout état de cause, la possibilité d'identifier des formules de conservation ciblée basées sur ces critères, utiles pour atteindre les objectifs susvisés, n'est pas à exclure. Il appartient au pouvoir législatif, dans chaque État membre ou pour l'ensemble de l'Union, de concevoir ces formules, qui respectent la protection des droits fondamentaux que la Cour garantit.

70 Arrêt Digital Rights Ireland e.a. (point 57), ainsi que arrêt Tele2 Sverige et Watson e.a. (point 105).

91. Il serait erroné de croire que la conservation ciblée de données afférentes à un public spécifique ou à une zone géographique déterminée est la seule formule que la Cour juge compatible avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte.

92. Il est possible, j'insiste, de trouver d'autres modalités de conservation ciblée des données, mis à part celles axées sur des groupes spécifiques de personnes ou des zones géographiques. De fait, les groupes de travail du Conseil que j'ai mentionnés ci-dessus sont de cet avis : ils ont notamment considéré, comme des pistes à explorer, la limitation des catégories de données conservées [71] ; la pseudonymisation des données [72] ; l'introduction de périodes de conservation limitées [73] ; l'exclusion de certaines catégories de fournisseurs de services de communications électroniques [74] ; les autorisations de conservation renouvelables [75] ; l'obligation de conserver les données dans l'Union ou le contrôle systématique et régulier, par une autorité administrative indépendante, des garanties offertes par les fournisseurs de services de communications électroniques contre l'utilisation abusive des données.

93. Selon moi, pour que la conservation des données soitcompatible avec la jurisprudence de la Cour, il convient de favoriser la conservation temporaire de certaines *catégories* de données relatives au trafic et de données de localisation, limitées en fonction de ce qui est strictement nécessaire pour atteindre l'objectif poursuivi, qui ne permettent pas, prises ensemble, d'obtenir une image précise et détaillée de la vie des personnes concernées.

94. En pratique, cela signifie que, pour les deux principales catégories (les données relatives au trafic et les données de localisation), seules les données *minimales* considérées comme absolument indispensables pour la prévention et le contrôle efficaces de la criminalité et pour la sauvegarde de la sécurité nationale devraient être conservées, au moyen de filtres appropriés.

95. Il appartient aux États membres ou aux institutions de l'Union de procéder à cet exercice de sélection par voie législative (avec l'aide de leurs propres experts), en renonçant à toute tentative d'imposer une conservation généralisée et indifférenciée de toutes les données relatives au trafic et données de localisation.

71 Les données qui ne sont pas strictement indispensables et objectivement nécessaires aux fins de la prévention et de la poursuite de la criminalité ainsi que de la sauvegarde de la sécurité publique seraient exclues de l'obligation de conservation. Il conviendrait notamment de préciser, en fonction de l'objectif poursuivi, les catégories de données relatives aux abonnés ou au trafic et de données de localisation qui devraient impérativement être conservées pour atteindre cet objectif. En particulier, les données qui ne sont pas jugées nécessaires pour les enquêtes et les poursuites pénales seraient exclues.

72 Méthode par laquelle les noms sont remplacés par un alias, de sorte que les données ne sont plus rattachées à un nom. Contrairement à l'anonymisation, la pseudonymisation permet de relier à nouveau les données au nom de la personne concernée.

73 On pourrait envisager de moduler les périodes de conservation en fonction des différentes catégories de données, en tenant compte de leur nature plus ou moins intrusive dans la vie privée des personnes. En outre, il conviendrait de prévoir que les données seront définitivement effacées à la fin de la période de conservation.

74 On pourrait envisager de ne pas imposer l'obligation de conserver des données à tous les fournisseurs de services de communications électroniques, mais d'introduire une telle obligation en fonction de leur taille et du type de services qu'ils offrent, en excluant, par exemple, ceux offrant des services hautement spécialisés.

75 Les régimes d'autorisation pourraient être fondés sur des évaluations périodiques des menaces dans chaque État membre. Il convient de garantir que le lien entre les données conservées et l'objectif poursuivi soit établi et adapté à la situation particulière de chaque État membre. Il serait par conséquent possible que les autorisations de conservation données aux fournisseurs donnent lieu à la conservation de différents types de données durant une période déterminée, en fonction de l'évaluation de la menace. Ces autorisations pourraient être accordées par un juge ou une autorité administrative indépendante et donneraient lieu à un examen périodique du caractère indispensable de cette conservation.

96. Outre cette limitation par catégorie, les données conservées ne peuvent l'être que pendant une certaine période, de sorte qu'elles ne permettent pas de donner une image détaillée de la vie des personnes concernées. Cette période de conservation doit également être adaptée en fonction de la nature des données, de sorte que celles qui fournissent des informations plus précises sur les modes de vie et les habitudes de ces personnes soient stockées pendant une période plus courte [76].

97. En d'autres termes, la différenciation de la période de conservation de chaque catégorie de données, en fonction de leur utilité pour atteindre les objectifs de sécurité, est une voie à explorer. En limitant la durée pendant laquelle les différentes catégories de données sont stockées simultanément (et peuvent donc être utilisées pour trouver des corrélations qui révèlent le mode de vie des personnes concernées), le droit garanti par l'article 8 de la Charte est davantage protégé.

98. Le CEPD s'est exprimé en ce sens lors de l'audience : plus les catégories de métadonnées conservées sont nombreuses et plus la période de conservation est longue, plus il est aisé de définir le profil détaillé d'une personne, et inversement [77].

99. Au demeurant, comme il a été souligné lors de l'audience, la frontière entre certaines métadonnées relatives aux communications électroniques et le contenu de ces mêmes communications est difficile à tracer. Certaines métadonnées peuvent être aussi révélatrices que le contenu même de ces communications, voire plus : tel peut être le cas des adresses (URL) des sites Internet visités [78]. Dès lors, il convient d'accorder une attention particulière à ce type de données et à d'autres données similaires, afin de circonscrire autant que possible la nécessité de leur conservation et la durée de celle-ci.

100. Il n'est pas facile de trouver une solution équilibrée, car la technique du recoupement et de la corrélation des données stockées permet aux services d'enquête et de surveillance d'identifier un suspect ou une menace, selon le cas. Néanmoins, il existe une différence de degré entre la conservation des données pour détecter ce suspect ou cette menace et celle qui permet d'obtenir un portrait détaillé de la vie d'une personne.

101. Dans l'attente d'une réglementation commune à l'ensemble de l'Union dans ce domaine spécifique, je ne pense pas que l'on puisse demander à la Cour d'assumer des fonctions réglementaires et de préciser, en détail, quelles catégories de données peuvent être conservées et pour combien de temps. Il appartient aux institutions de l'Union et aux États membres, une fois fixées les limites qui, selon la Cour, découlent de la Charte, de placer le curseur au bon endroit afin d'opérer un équilibre entre la sauvegarde de la sécurité et les droits fondamentaux protégés par la Charte.

76 Tel est, semble-t-il, le régime appliqué en Allemagne, dont le gouvernement a indiqué lors de l'audience que, en vertu de sa législation, la période de conservation des données relatives au trafic est de dix semaines, tandis qu'elle est de quatre semaines seulement pour les données de localisation. En revanche, la République française estime qu'une période de conservation d'un an des données relatives au trafic et des données de localisation est indispensable. Selon cet État membre, la réduction de cette période à moins d'un an aurait pour effet de diminuer l'efficacité des services de police judiciaire.

77 Bien entendu, il convient de garantir que les fournisseurs de services de communications électroniques effacent définitivement les données à la fin de la période de conservation (à l'exception des données qui peuvent continuer à être stockées à des fins commerciales, conformément à la directive 2002/58).

78 Au cours de l'audience, le gouvernement français a déclaré que les URL étaient exclues des données de connexion pour lesquelles sa législation prévoit une obligation générale de conservation.

102. Il est vrai que renoncer à des informations pouvant être déduites d'un plus grand nombre de données conservées pourrait, dans certains cas, rendre plus difficile la lutte contre les menaces potentielles. Cependant, c'est un prix, parmi d'autres, que les pouvoirs publics doivent payer lorsqu'ils s'imposent à eux-mêmes l'obligation de sauvegarder les droits fondamentaux.

103. De même que personne ne préconiserait une obligation ex ante de conservation généralisée et indifférenciée du *contenu* des communications électroniques privées (même si la loi garantissait le caractère restreint de l'accès ultérieur audit contenu), les métadonnées de ces communications, qui peuvent révéler des informations aussi sensibles que le contenu lui-même, ne devraient pas pouvoir faire l'objet d'une conservation indifférenciée et généralisée.

104. La difficulté législative – que je reconnais – de définir précisément les hypothèses et les conditions dans lesquelles une conservation ciblée peut être effectuée ne justifie pas que les États membres, en faisant de l'exception une règle, érigent la conservation généralisée des données personnelles en principe central de leur législation. Si tel était le cas, une atteinte importante d'une durée indéterminée au droit à la protection des données à caractère personnel serait admise.

105. Je dois ajouter que rien ne s'oppose à ce que, dans des situations réellement *exceptionnelles*, caractérisées par une menace imminente ou par un risque extraordinaire justifiant la constatation officielle de la situation d'urgence dans un État membre, la législation nationale prévoie, pour une durée limitée, la possibilité d'imposer une obligation de conservation de données aussi étendue et générale qu'il est jugé indispensable.

106. Dans ce contexte, il serait possible d'adopter une réglementation permettant expressément une conservation des données (et l'accès à celles-ci) plus étendue, dans le cadre de conditions et de procédures garantissant le caractère extraordinaire de ces mesures, quant à leur portée matérielle et temporelle, assorties de garanties juridictionnelles correspondantes.

107. Un examen comparatif des régimes normatifs qui gouvernent les situations constitutionnelles d'urgence montre qu'il n'est pas impossible de délimiter les hypothèses factuelles pouvant entraîner l'application d'un régime normatif particulier, en prévoyant quelle autorité peut adopter cette décision, dans quelles conditions et sous quel contrôle [79].

E. Les réponses spécifiques aux trois questions préjudicielles

1. Considération liminaire

108. La juridiction de renvoi demande d'interpréter l'article 15, paragraphe 1, de la directive 2002/58 en lien avec plusieurs droits garantis par la Charte : le droit au respect de la vie privée et familiale (article 7), le droit à la protection des données à caractère personnel (article 8) et le droit à la liberté d'expression et d'information (article 11).

109. Comme je l'indique dans les conclusions présentées dans les affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a., il s'agit effectivement des droits qui, selon la Cour, pourraient être affectés dans de tels cas.

[79] Ackerman, B., « The Emergency Constitution », *Yale Law Journal*, vol. 113, 2004, p. 1029 à 1092 ; Ferejohn, J., et Pasquino, P., « The Law of the Exception : A Typology of Emergency Powers », *International Journal of Constitutional Law*, vol. 2, 2004, p. 210 à 239.

110. Toutefois, la Cour constitutionnelle renvoie également aux articles 4 et 6 de la Charte, auxquels se réfèrent respectivement la deuxième et la première question préjudicielle.

111. En ce qui concerne l'article 6 de la Charte, qui garantit le droit à la liberté et à la sûreté, il a également été invoqué dans les affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a., et je me suis prononcé sur sa pertinence dans les conclusions y afférentes, auxquelles je renvoie [80].

112. Quant à l'article 4 de la Charte, étant donné que la réponse ne dépend pas tant de l'analyse de la législation nationale, afin de la confronter avec le droit de l'Union, que de l'interprétation de cette disposition, il me semble opportun d'y répondre en premier lieu.

2. La deuxième question préjudicielle

113. La référence à l'interdiction de la torture et des peines ou traitements inhumains ou dégradants, garantie par l'article 4 de la Charte, est en effet exclusive à ce renvoi préjudiciel, ce qui m'oblige à y prêter attention.

114. En invoquant l'article 4 de la Charte, la juridiction de renvoi souhaite souligner que la réglementation nationale vise également à remplir l'*obligation positive* qui incombe à l'autorité publique d'établir « 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 » [81].

115. À mon sens, cette *obligation positive* concrète n'est pas très différente de chacune des obligations spécifiques qui matérialisent, pour l'État, la proclamation d'un catalogue de droits fondamentaux. Les droits à la vie (article 2 de la Charte), à l'intégrité physique (article 3 de la Charte) ou à la protection des données (article 8 de la Charte), ainsi que les libertés d'expression (article 11 de la Charte) ou de pensée, de conscience et de religion (article 10 de la Charte), comportent pour l'État l'obligation d'établir un cadre normatif dans lequel leur jouissance effective est garantie, le cas échéant par l'usage de la force qui est le monopole de l'autorité publique, contre quiconque tenterait de l'empêcher ou de l'entraver [82].

116. En ce qui concerne l'abus sexuel des mineurs, la Cour européenne des droits de l'homme considère que les enfants et autres personnes vulnérables ont un droit renforcé à la protection de l'État, au moyen de l'adoption de règles de droit pénal qui sanctionnent de manière efficace et dissuasive la commission de telles infractions [83].

117. Ce droit renforcé à la protection ne trouve pas son fondement seulement dans l'article 4 de la Charte, puisque l'article 1er (dignité humaine) ou l'article 3 (droit à l'intégrité physique et mentale) pourraient naturellement être invoqués.

80 Conclusions dans les affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a. (points 95 et suiv).

81 Libellé de la deuxième question in fine. Cette allusion aux moyens de communication électronique explique pourquoi la question mentionne une deuxième *obligation positive* pesant sur les États, celle imposée par l'article 8 de la Charte en matière de protection des données à caractère personnel. Le double renvoi à l'article 8 de la Charte révèle que la juridiction de renvoi attribue aux droits garantis par la Charte, selon leur nature, une double fonction : celle de *limite* à l'obligation litigieuse et celle de *justification* de cette obligation.

82 Cette obligation d'efficacité se traduit par une obligation de résultat pour l'autorité publique dans l'État social ou providence, dans lequel, au-delà de la reconnaissance formelle des droits, la réalisation pratique de leur contenu matériel importe.

83 Cour EDH, 2 décembre 2008, K.U. c. Finlande, CE:ECHR:2008:1202JUD000287202, § 46.

118. Bien que l'obligation positive des autorités publiques d'assurer la protection des enfants et autres personnes vulnérables ne puisse être ignorée dans l'appréciation des intérêts juridiques affectés par la réglementation nationale [84], elle ne saurait non plus se traduire par un « fardeau excessif » pour l'autorité publique [85], ni être remplie au mépris de la légalité ou du respect des autres droits fondamentaux [86].

3. La première question préjudicielle

119. En somme, la juridiction de renvoi souhaite savoir si le droit de l'Union s'oppose à la loi nationale sur laquelle elle est appelée à statuer dans le cadre d'un recours en annulation fondé sur l'inconstitutionnalité de cette loi.

120. La Cour ayant déjà fourni l'interprétation de la directive 2002/58 conforme aux dispositions afférentes de la Charte, la réponse à la question préjudicielle devra tenir compte de la jurisprudence établie dans l'arrêt Tele2 Sverige et Watson e.a., le cas échéant avec les nuances qui suivent.

121. Partant de cette prémisse, les clés d'interprétation qui peuvent être fournies à la Cour constitutionnelle pour qu'elle apprécie elle-même la conformité au droit de l'Union de la réglementation interne doivent porter, tour à tour, sur la conservation et l'accès aux données, comme le prévoit cette réglementation nationale.

a) Les conditions de la conservation des données

122. Le gouvernement belge souligne qu'il souhaitait établir un cadre juridique clair, avec les garanties nécessaires à la protection de la vie privée, plutôt que de s'appuyer sur la pratique des opérateurs de services de communications électroniques en matière de conservation des données aux fins de facturation et de traitement des demandes d'informations des clients.

123. D'après ledit gouvernement, l'obligation générale et préventive de conservation de données n'a pas seulement pour but l'instruction, la recherche et la poursuite de faits de criminalité grave, mais aussi la sauvegarde de la sécurité nationale, 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'usages interdits de systèmes de communications électroniques [87] ou la réalisation d'un autre objectif identifié à l'article 23, premier alinéa, du règlement 2016/679.

84 À cet égard, je considère qu'aux droits invoqués par la juridiction de renvoi (en tant que *limites* et non que *justification* de l'obligation en cause) pourraient s'ajouter le droit à une protection juridictionnelle effective (article 47 de la Charte) ou les droits de la défense (article 48 de la Charte), dont l'éventuelle violation a également été débattue dans les procédures au principal. Néanmoins, le dispositif de la décision de renvoi se réfère uniquement aux articles 7, 8, 11 et à l'article 52, paragraphe 1, de la Charte.

85 Cour EDH, 28 octobre 1998, Osman c. Royaume-Uni, CE:ECHR:1998:1028JUD002345294, § 116.

86 Cour EDH, 28 octobre 1998, Osman c. Royaume-Uni, CE:ECHR:1998:1028JUD002345294, § 116 in fine : « [il est nécessaire] de s'assurer que la police exerce son pouvoir de juguler et de prévenir la criminalité en respectant pleinement les voies légales et autres garanties qui limitent légitimement l'étendue de ses actes d'investigations criminelles et de traduction des délinquants en justice, y compris les garanties figurant aux articles 5 et 8 de la Convention ». Voir, également, Cour EDH, 2 décembre 2008, K.U. c. Finlande, CE:ECHR:2008:1202JUD000287202, § 48. Dans le même ordre d'idées, au point 49 de l'arrêt du 29 juillet 2019, Gambino et Hyka (C-38/18, EU:C:2019:628), la Cour a jugé que les droits en faveur de la victime ne sauraient affecter la jouissance effective des droits reconnus à la personne poursuivie.

87 Elle est aussi motivée par la volonté de pouvoir donner suite à un appel vers un service d'urgence ou pour retrouver une personne disparue dont l'intégrité physique est en danger imminent.

124. Selon le gouvernement belge :

– en tant que telle, la conservation des données ne permet pas de tirer des conclusions très précises à propos de la vie privée des personnes concernées : la possibilité de tirer de telles conclusions n'interviendrait que dans la mesure où il serait également donné accès aux données conservées ;

– la loi contient des sauvegardes en vue de protéger la vie privée ; entre autres, la conservation des données ne concerne pas le contenu des communications ; les garanties en ce qui concerne notamment la justification de la conservation, le droit de regard et le droit à la rectification sont intégralement applicables ; les fournisseurs et les opérateurs doivent soumettre les données conservées aux mêmes obligations et mesures de sécurité et de protection que celles applicables aux données sur le réseau, en empêchant leur destruction accidentelle ou illicite, leur perte ou leur altération accidentelle ;

– les données peuvent être conservées durant 12 mois (après quoi elles doivent être détruites) et seulement sur le territoire de l'Union ;

– les fournisseurs et opérateurs mettent en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, illisibles et inutilisables par toute personne qui n'est pas autorisée à y avoir accès ;

– en tout état de cause, ces opérations sont effectuées sous la tutelle du régulateur des secteurs des postes et des télécommunications belge et de l'Autorité de protection des données.

125. En dépit de ces garanties, il est vrai que la législation belge impose aux opérateurs et aux fournisseurs de services de communications électroniques l'obligation, générale et indifférenciée, de conserver les données relatives au trafic et les données de localisation, au sens de la directive 2002/58, traitées dans le cadre de la fourniture de ces services. Comme indiqué ci-dessus, la période de conservation est en général de douze mois : aucune limite de temps n'est prévue en fonction des catégories de données conservées.

126. Cette obligation de conservation générale et indifférenciée s'applique de manière permanente et continue. Bien que son objectif soit la prévention, la recherche et la poursuite de tous les types d'infractions (depuis celles liées à la sécurité nationale ou à la défense, ou les infractions particulièrement graves, jusqu'à celles pouvant entraîner une peine d'emprisonnement inférieure à un an), une telle obligation n'est pas conforme à la jurisprudence de la Cour et ne peut donc être considérée comme compatible avec la Charte.

127. Pour s'adapter à cette jurisprudence, le législateur belge devra explorer d'autres voies (telles que celles mentionnées ci-dessus) qui établissent des formules de conservation limitée. Ces formules, variables selon les catégories de données, doivent respecter le principe selon lequel seul le *minimum* de données requises doit être conservé, en fonction du risque ou de la menace, et ce pour une durée limitée, qui dépendra de la nature des informations stockées. En tout état de cause, la conservation ne saurait fournir une *cartographie* précise de la vie privée, des habitudes, des comportements ou des relations sociales des personnes concernées.

b) Les conditions d'accès des autorités publiques aux données conservées

128. Selon moi, les conditions énoncées dans l'arrêt Tele2 Sverige et Watson e.a.[88] demeurent pertinentes concernant l'accès : la réglementation nationale doit établir les conditions matérielles et procédurales régissant l'accès des autorités nationales compétentes aux données conservées[89].

129. Le gouvernement belge précise que l'article 126, § 2, de la loi de 2005[90] énumère limitativement les autorités nationales qui peuvent recevoir les données conservées conformément au § 1 du même article.

130. Celles-ci comprennent les autorités judiciaires à proprement parler et le ministère public ; la Sûreté de l'État ; le Service Général du Renseignement et de la Sécurité, sous le contrôle de deux commissions indépendantes ; les officiers de police judiciaire de l'Institut belge des services postaux et des télécommunications ; les services d'urgence ; les officiers de police judiciaire de la Cellule des personnes disparues de la Police Fédérale ; le Service de médiation pour les télécommunications et l'autorité de surveillance du secteur financier.

131. De manière générale, le gouvernement belge affirme que la législation nationale ne permet pas aux différents services d'avoir accès aux données afin de poursuivre activement des menaces non identifiées ou sans indications concrètes. Les autorités nationales ne pourraient donc tout simplement pas accéder à des données de communication brutes et traiter automatiquement ces données afin d'en tirer des renseignements et de prévenir activement les dangers pour la sécurité.

132. Selon le même gouvernement, l'accès aux données est soumis à des conditions strictes, en fonction du statut de chacune des autorités nationales compétentes.

133. La réponse à la première question préjudicielle ne requiert pas, à mon sens, que la Cour procède à une analyse exhaustive des conditions dans lesquelles chacune de ces autorités peut obtenir les données conservées. Cette tâche incombe plutôt à la juridiction de renvoi, qui devra l'accomplir à la lumière des orientations données dans la jurisprudence issue des arrêts Tele2 Sverige et Watson e.a. et Ministerio Fiscal.

134. Au demeurant, selon les informations fournies par le gouvernement belge, il existe des différences notables entre les conditions d'accès concernant les autorités judiciaires ou le ministère public[91], en vue de la recherche, de l'instruction et de la poursuite d'infractions, aux termes des articles 46 bis[92] et 88 bis[93] du code d'instruction criminelle, et celles qui s'appliquent aux autres autorités.

88 Voir point 60 des présentes conclusions.

89 Arrêt Tele2 Sverige et Watson e.a. (point 118).

90 Article 126, dans le libellé résultant de la loi du 29 mai 2016.

91 L'adéquation du ministère public pour prendre des mesures de ce type est débattue dans le cadre du renvoi préjudiciel dans l'affaire pendante Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18).

92 La compétence pour requérir des données d'identification de la part des opérateurs appartient au ministère public, par décision motivée et écrite (verbale en cas d'urgence), qui démontre le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête. Pour des infractions qui ne sont pas de nature à entraîner un emprisonnement principal d'un an ou une peine plus lourde, le ministère public ne peut requérir les données que pour une période de six mois préalable à sa décision.

93 La compétence pour requérir des opérateurs le suivi des communications électroniques ou les données relatives au trafic et les données de localisation conservées appartient au juge d'instruction. Il peut prendre cette mesure s'il existe des indices sérieux de la commission d'une infraction passible de certaines peines, par ordonnance motivée et écrite (verbale en cas d'urgence) soumise aux mêmes exigences de proportionnalité et de subsidiarité que celles applicables au ministère public. Il existe quelques exceptions lorsque la mesure vise certaines catégories professionnelles protégées (par exemple, les avocats ou les médecins).

135. S'agissant des services de renseignement et de sécurité, conformément à la loi de 1998, la demande d'accès aux données relatives au trafic et aux données de localisation doit se fonder sur des critères objectifs qui garantissent que l'accès est limité à ce qui est strictement nécessaire, sur la base d'une menace préalablement identifiée [94]. Des délais d'accès différents (six, neuf ou douze mois) sont prévus en fonction de la menace potentielle et la demande doit respecter les principes de subsidiarité et de proportionnalité. En outre, un mécanisme de contrôle par une autorité indépendante a été mis en place [95].

136. Concernant les officiers de police judiciaire de l'Institut belge des services postaux et des télécommunications, leur accès aux données détenues par les opérateurs télécom n'est possible que dans des cas bien précis et fortement limités [96], sans que, selon le gouvernement belge, leur activité ne touche aux particuliers dont les données sont conservées.

137. En ce qui concerne les services d'urgence offrant de l'aide sur place, ils peuvent demander les données de l'auteur d'un appel d'urgence lorsque, à la suite de cet appel, ils n'obtiennent pas du fournisseur ou de l'opérateur concerné les données d'identification de l'intéressé ou obtiennent des données incomplètes ou incorrectes.

138. S'agissant des officiers de police judiciaire de la Cellule des personnes disparues de la Police Fédérale, ils peuvent exiger de l'opérateur les données nécessaires pour retrouver une personne disparue dont l'intégrité physique est en danger imminent. L'accès, soumis à des conditions strictes, est limité aux données permettant d'identifier l'utilisateur et à celles relatives à l'accès et à la connexion des terminaux au réseau et au service, ainsi qu'à la localisation de ces équipements, et se limite aux données qui ont été conservées dans les 48 heures précédant la demande.

139. Quant au Service de médiation pour les télécommunications, il peut seulement demander les données d'identification de la personne ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques. Dans ce cas, il n'y a pas de contrôle préalable par une autorité judiciaire ou administrative indépendante (autre que le Service lui-même).

140. Enfin, afin de lutter contre la criminalité financière, l'autorité de surveillance du secteur financier peut avoir accès aux données relatives au trafic et aux données de localisation, sous réserve de l'autorisation préalable du juge d'instruction.

141. L'exposé de ces modalités et conditions d'accès aux données conservées, qui valent pour chacune des autorités autorisées à les obtenir, met en évidence une variété d'hypothèses et de sauvegardes dont l'analyse détaillée au regard des critères formulés par la Cour dans sa jurisprudence [97] appartient à la juridiction de renvoi.

94 La décision mentionne, selon le cas, les personnes physiques ou morales, les associations de fait ou les groupements, les objets, les lieux, les événements ou les informations soumis à la méthode spécifique. Elle doit aussi mentionner le rapport existant entre l'objet des données requises et la menace potentielle qui justifie cette méthode particulière.

95 La Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité (Commission BIM) et le Comité permanent de contrôle des services de renseignement (Comité R). Le gouvernement belge déclare que la Commission BIM est responsable du suivi des méthodes de recherche employées par les services de renseignement et de sécurité, et exerce à cet égard un contrôle de première ligne. Cette commission, composée de magistrats, exerce ses missions de contrôle de manière totalement indépendante. Un contrôle indépendant de deuxième ligne, exercé par le Comité R, est également organisé.

96 Il est permis pour la recherche, l'instruction ou la poursuite d'infractions aux articles 114 (sécurité des réseaux), 124 (confidentialité des communications électroniques) et 126 (conservation de données et accès à celles-ci) de la loi de 2005.

97 Je renvoie au point 60 des présentes conclusions.

142. Je note, par exemple, que, dans le contexte de la législation en cause, il ne semble pas que les autorités nationales compétentes aient systématiquement l'obligation d'informer les personnes concernées (pour autant que cette communication ne compromette pas les enquêtes en cours) que leurs données ont été consultées. Il ne semble pas non plus que, du moins dans certains cas, comme ceux relatifs aux infractions financières, des règles prédéterminées sur la gravité de ces infractions soient établies pour justifier l'accès aux données pertinentes. La relation entre l'intensité de l'ingérence et la gravité de l'infraction visée par l'enquête, au sens de l'arrêt Ministerio Fiscal, n'apparaît pas dans toutes les hypothèses.

143. Quoi qu'il en soit, je suis d'avis que les considérations liées à l'accès des autorités aux données passent au second plan dès lors que, au vu de ce qui précède, la conservation généralisée et indifférenciée de ces données est elle-même la principale raison pour laquelle la législation nationale sur laquelle porte le présent renvoi préjudiciel n'est pas conforme au droit de l'Union.

4. La troisième question préjudicielle

144. La Cour constitutionnelle souhaite savoir si, dans l'hypothèse où, à la lumière de la réponse de la Cour, il était établi que la législation nationale est incompatible avec le droit de l'Union, elle pourrait maintenir provisoirement les effets de cette réglementation. Cela éviterait l'insécurité juridique et permettrait que les données collectées et conservées continuent d'être utilisées aux fins des objectifs poursuivis.

145. Selon une jurisprudence constante, « 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 ». Si « des juridictions nationales avaient le pouvoir de donner aux dispositions nationales la primauté par rapport au droit de l'Union contraire à celles-ci, serait-ce même à titre provisoire, il serait porté atteinte à l'application uniforme du droit de l'Union »[98].

146. La Commission estime que, la Cour n'ayant pas limité dans le temps les effets de l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58, la réponse à cette question de la juridiction de renvoi devrait être négative[99].

147. Cependant, dans l'arrêt du 28 février 2012, Inter-Environnement Wallonie et Terre wallonne[100], la Cour a relevé que, devant l'existence d'une considération impérieuse liée à la protection de l'environnement, une juridiction nationale pouvait exceptionnellement être autorisée à faire usage d'une disposition nationale l'habilitant à maintenir certains effets d'un acte national annulé pour méconnaissance d'une règle de l'Union[101].

98 Arrêt du 28 juillet 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603, point 33).

99 Point 100 des observations écrites de la Commission.

100 C-41/11, EU:C:2012:103.

101 Arrêt du 28 février 2012, Inter-Environnement Wallonie et Terre wallonne (C-41/11, EU:C:2012:103, point 58). Au point 34 de l'arrêt du 28 juillet 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603), la Cour a déduit de cette affirmation qu'elle avait « entendu reconnaître, au cas par cas et à titre exceptionnel, à une juridiction nationale la faculté d'aménager les effets de l'annulation d'une disposition nationale jugée incompatible avec le droit de l'Union ».

148. Cette jurisprudence a été confirmée par l'arrêt du 29 juillet 2019, Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen [102]. Qu'elle soit établie dans le domaine de la protection de l'environnement ou fondée sur la sécurité de l'approvisionnement en électricité, je ne vois aucune raison d'exclure son application dans d'autres domaines du droit de l'Union, en particulier dans celui qui nous occupe ici.

149. Si une « considération impérieuse liée à la protection de l'environnement » peut justifier que, exceptionnellement, les juridictions nationales préservent certains effets d'une disposition nationale incompatible avec le droit de l'Union, c'est parce que la protection de l'environnement représente « l'un des objectifs essentiels de l'Union et revêt un caractère tant transversal que fondamental » [103].

150. Or, parmi les objectifs de l'Union figure également la constitution d'un espace de sécurité (article 3 TUE) incluant le respect des fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer l'ordre public et de sauvegarder la sécurité nationale (article 4, paragraphe 2, TUE). Il s'agit là d'un objectif non moins « transversal et fondamental » que la protection de l'environnement, car sa réalisation est la condition nécessaire pour la mise en place d'un cadre normatif propre à garantir la jouissance effective des droits et libertés fondamentaux.

151. Selon moi, des raisons impérieuses liées à la protection de la sécurité nationale pourraient justifier que, en l'espèce, la Cour autorise exceptionnellement la juridiction de renvoi à maintenir, à tout le moins, certains effets de la loi en cause.

152. Ce maintien supposerait que, à la lumière des constatations de la Cour, la juridiction de renvoi considère la réglementation nationale comme incompatible avec le droit de l'Union et juge extrêmement perturbatrices les répercussions que son annulation immédiate (si l'annulation était la conséquence attachée par le droit national à cette incompatibilité) ou sa non-application pourraient entraîner pour la sécurité publique ou la sûreté de l'État.

153. La subsistance provisoire (de tout ou partie) des effets de la réglementation nationale exigerait en outre :

– que la finalité de cette prorogation soit d'éviter un vide normatif ayant des effets aussi pernicieux que ceux résultant de l'application de la réglementation litigieuse, vide qu'il serait impossible de combler par d'autres moyens et qui priverait les autorités nationales d'un instrument précieux pour garantir la sûreté de l'État ; et

– qu'elle dure le laps de temps strictement nécessaire pour adopter des mesures permettant de remédier à l'incompatibilité constatée avec le droit de l'Union [104].

154. Plaident en faveur de cette solution, en outre, la difficulté de mettre en conformité les réglementations nationales avec la jurisprudence établie dans l'arrêt Tele2 Sverige et Watson e.a. [105] et le fait que le législateur belge a manifesté sa volonté de se conformer à l'arrêt Digital Rights Ireland e.a. en modifiant sa propre législation. Ce précédent donne à penser qu'il adaptera également la loi du 29 mai 2016 (adoptée avant que l'arrêt Tele2 Sverige et Watson e.a. ne soit connu) à la jurisprudence établie dans ce dernier.

102 C-411/17, EU:C:2019:622 (point 178).

103 Arrêt du 28 février 2012, Inter-Environnement Wallonie et Terre wallonne (C-41/11, EU:C:2012:103, point 57).

104 Arrêt du 28 février 2012, Inter-Environnement Wallonie et Terre wallonne (C-41/11, EU:C:2012:103, point 62).

105 Point 45 des observations écrites du gouvernement danois.

V. Conclusion

155. Compte tenu de ce qui précède, je propose que la Cour réponde à la Cour constitutionnelle (Belgique) comme suit :

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), lu en combinaison avec les articles 7, 8, 11 et l'article 52, paragraphe l, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que :

   – il s'oppose à une législation nationale imposant aux opérateurs et aux fournisseurs de services de communications électroniques l'obligation de conserver, de manière générale et indifférenciée, les données relatives au trafic et les données de localisation de tous les abonnés et utilisateurs, pour tous les moyens de communication électronique ;

   – il est à cet égard indifférent que cette législation nationale ait pour objectifs non seulement la recherche, la découverte et la poursuite d'infractions graves ou non, mais aussi la sécurité nationale, la défense du territoire, la sécurité publique, la prévention de l'utilisation non autorisée du système de communications électroniques, ou tout autre objectif prévu à l'article 23, paragraphe 1, du règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;

   – il est à cet égard indifférent que l'accès aux données conservées soit soumis à des garanties précisément réglementées. Il appartient à la juridiction de renvoi de vérifier si la législation nationale qui régit les conditions de cet accès par les autorités compétentes le limite à des cas spécifiques dont la gravité rend indispensable l'ingérence ; le soumet au contrôle préalable (sauf cas d'urgence) d'une juridiction ou d'une autorité indépendante ; et prévoit que les personnes concernées sont informées de cet accès, pour autant que cette communication ne compromette pas l'action desdites autorités.

2) Les articles 4 et 6 de la charte des droits fondamentaux n'affectent pas l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58, lu en combinaison avec les autres articles susmentionnés de ladite charte, d'une manière qui empêcherait de constater l'incompatibilité d'une législation nationale telle que celle en cause au principal avec le droit de l'Union.

3) Une juridiction nationale peut, si le droit interne le permet, maintenir exceptionnellement et provisoirement les effets d'une législation, telle que celle en cause au principal, même si elle est incompatible avec le droit de l'Union, si ce maintien est justifié par des considérations impérieuses liées à des menaces pour la sécurité publique ou nationale auxquelles d'autres moyens ou solutions de substitution ne permettraient pas de parer. Ce maintien ne peut durer que le temps strictement nécessaire pour remédier à l'incompatibilité susvisée avec le droit de l'Union.