CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. MACIEJ SZPUNAR
présentées le 27 octobre 2022 (1)

Affaire C 470/21

La Quadrature du Net,
Fédération des fournisseurs d'accès à Internet associatifs,
Franciliens.net,
French Data Network
contre
Premier ministre,
Ministère de la Culture

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

« Renvoi préjudiciel – Traitement des données à caractère personnel et protection de la vie privée dans le secteur des communications électroniques – Directive 2002/58/CE – Article 15, paragraphe 1 – Faculté pour les États membres de limiter la portée de certains droits et obligations – Obligation de contrôle préalable par une juridiction ou une entité administrative indépendante dotée d'un pouvoir contraignant – Données d'identité civile correspondant à une adresse IP »

I. Introduction

1. La question de la conservation et de l'accès à certaines données des utilisateurs de l'internet est une question d'une actualité permanente et fait l'objet d'une jurisprudence récente mais déjà abondante de la Cour.

2. La présente affaire offre à la Cour l'occasion de traiter une nouvelle fois cette question, dans le contexte renouvelé de la lutte contre les infractions aux droits de propriété intellectuelle commises exclusivement en ligne.

II. Le cadre juridique

A. Le droit de l'Union

3. Les considérants 2, 6, 7, 11, 22, 26 et 30 de la directive 2002/58/CE (2) énoncent :

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

[...]

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

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

[...]

(11) À l'instar de la directive [95/46/CE (3)], la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit communautaire. Elle ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles visées à l'article 15, paragraphe 1, de la présente directive, nécessaires pour la protection de la sécurité publique, de la défense, de la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des États membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales [, signée à Rome le 4 novembre 1950], telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. Lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique. Elles devraient également être subordonnées à des garanties appropriées, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

[...]

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

[...]

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

[...]

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

4. Aux termes de l'article 2 de cette directive, intitulé « Définitions » :

« [...]

Les définitions suivantes sont aussi applicables :

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

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

c) "données de localisation" : toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement

terminal d'un utilisateur d'un service de communications électroniques accessible au public ;

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

[...] »

5. L'article 3 de ladite directive, intitulé « Services concernés », dispose :

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

6. L'article 5 de la même directive, intitulé « Confidentialité des communications », prévoit :

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

[...]

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

7. Aux termes de l'article 6 de la directive 2002/58, intitulé « Données relatives au trafic » :

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

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

[...] »

8. L'article 15, paragraphe 1, de cette directive 2002/58, intitulé « Application de certaines dispositions de la directive [95/46] », énonce :

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

B. Le droit français

1. Le code de la propriété intellectuelle

9. L'article L. 331 12 du code de la propriété intellectuelle, dans sa version applicable au litige au principal (ci-après le « CPI »), dispose :

« La Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet [ci-après la "Hadopi"] est une autorité publique indépendante. »

10. L'article L. 331 13 du CPI prévoit :

« La [Hadopi] assure :

[...]

2° Une mission de protection [des œuvres et objets auxquels est attaché un droit d'auteur ou un droit voisin sur les réseaux de communications électroniques] à l'égard des atteintes à ces droits commises sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne ; [...] »

11. Aux termes de l'article L. 331-15 de ce code :

« La [Hadopi] est composée d'un collège et d'une commission de protection des droits. [...]

[...]

Dans l'exercice de leurs attributions, les membres du collège et de la commission de protection des droits ne reçoivent d'instruction d'aucune autorité. »

12. L'article L. 331 17 dudit code dispose :

« La commission de protection des droits est chargée de prendre les mesures prévues à l'article L. 331-25. »

13. Aux termes de l'article L. 331 21 du même code :

« Pour l'exercice, par la commission de protection des droits, de ses attributions, la [Hadopi »] dispose d'agents publics assermentés habilités par [son] président dans des conditions fixées par un décret en Conseil d'État. [...]

Les membres de la commission de protection des droits et les agents mentionnés au premier alinéa reçoivent les saisines adressées à ladite commission dans les conditions prévues à l'article L. 331 24. Ils procèdent à l'examen des faits.

Ils peuvent, pour les nécessités de la procédure, obtenir tous documents, quel qu'en soit le support, y compris les données conservées et traitées par les opérateurs de communications électroniques en application de l'article L. 34 1 du code des postes et des communications électroniques et les prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Ils peuvent également obtenir copie des documents mentionnés à l'alinéa précédent.

Ils peuvent, notamment, obtenir des opérateurs de communications électroniques l'identité, l'adresse postale, l'adresse électronique et les coordonnées téléphoniques de l'abonné dont l'accès à des services de communication au public en ligne a été utilisé à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés sans l'autorisation des titulaires des droits [...] lorsqu'elle est requise. »

14. L'article L. 331 24 du CPI dispose :

« La commission de protection des droits agit sur saisine d'agents assermentés et agréés [...] qui sont désignés par :

– les organismes de défense professionnelle régulièrement constitués ;

– les organismes de gestion collective ;

– le Centre national du cinéma et de l'image animée.

La commission de protection des droits peut également agir sur la base d'informations qui lui sont transmises par le procureur de la République.

Elle ne peut être saisie de faits remontant à plus de six mois. »

15. Aux termes de l'article L. 331 25 de ce code, disposition régissant la procédure dite de « réponse graduée » :

« Lorsqu'elle est saisie de faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336 3 [du CPI], la commission de protection des droits peut envoyer à l'abonné [...] une recommandation lui rappelant les dispositions de l'article L. 336 3, lui enjoignant de respecter l'obligation qu'elles définissent et l'avertissant des sanctions encourues en application des articles L. 335 7 et L. 335 7 1. Cette recommandation contient également une information de l'abonné sur l'offre légale de contenus culturels en ligne, sur l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336 3 ainsi que sur les dangers pour le renouvellement de la création artistique et pour l'économie du secteur culturel des pratiques ne respectant pas le droit d'auteur et les droits voisins.

En cas de renouvellement, dans un délai de six mois à compter de l'envoi de la recommandation visée au premier alinéa, de faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336 3, la commission peut adresser une nouvelle recommandation comportant les mêmes informations que la précédente par la voie électronique [...] Elle doit assortir cette recommandation d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation de cette recommandation.

Les recommandations adressées sur le fondement du présent article mentionnent la date et l'heure auxquelles les faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336-3 ont été constatés. En revanche, elles ne divulguent pas le contenu des œuvres ou objets protégés concernés par ce manquement. Elles indiquent les coordonnées téléphoniques, postales et électroniques où leur destinataire peut adresser, s'il le souhaite, des observations à la commission de protection des droits et obtenir, s'il en formule la demande expresse, des précisions sur le contenu des œuvres ou objets protégés concernés par le manquement qui lui est reproché. »

16. L'article L. 331 29 dudit code dispose :

« Est autorisée la création, par la [Hadopi], d'un traitement automatisé de données à caractère personnel portant sur les personnes faisant l'objet d'une procédure dans le cadre de la présente sous-section.

Ce traitement a pour finalité la mise en œuvre, par la commission de protection des droits, des mesures prévues à la présente sous-section, de tous les actes de procédure afférents et des modalités de l'information des organismes de défense professionnelle et des organismes de gestion collective des éventuelles saisines de l'autorité judiciaire ainsi que des notifications prévues au cinquième alinéa de l'article L. 335 7.

Un décret [...] fixe les modalités d'application du présent article. Il précise notamment :

– les catégories de données enregistrées et leur durée de conservation ;

– les destinataires habilités à recevoir communication de ces données, notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne ;

– les conditions dans lesquelles les personnes intéressées peuvent exercer, auprès de la [Hadopi], leur droit d'accès aux données les concernant [...] »

17. L'article R. 331 37 du même code prévoit :

« Les opérateurs de communications électroniques [...] et les prestataires [...] sont tenus de communiquer, par une interconnexion au traitement automatisé de données à caractère personnel mentionné à l'article L. 331 29 ou par le recours à un support d'enregistrement assurant leur intégrité et leur sécurité, les données à caractère personnel et les informations mentionnées au 2° de l'annexe du [décret n° 2010 236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331 29 du [CPI] dénommé « Système de gestion des mesures pour la protection des œuvres sur Internet » (4)] [...] dans un délai de huit jours suivant la transmission par la commission de protection des droits des données techniques nécessaires à l'identification de l'abonné dont l'accès à des services de communication au public en ligne a été utilisé à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés sans l'autorisation des titulaires des droits [...] lorsqu'elle est requise.

[...] »

18. L'article R. 335 5 du CPI dispose :

« I.- Constitue une négligence caractérisée, punie de l'amende prévue pour les contraventions de la cinquième classe, le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne, lorsque se trouvent réunies les conditions prévues au II :

1° Soit de ne pas avoir mis en place un moyen de sécurisation de cet accès ;

2° Soit d'avoir manqué de diligence dans la mise en œuvre de ce moyen.

II.- Les dispositions du I ne sont applicables que lorsque se trouvent réunies les deux conditions suivantes :

1° En application de l'article L. 331 25 et dans les formes prévues par cet article, le titulaire de l'accès s'est vu recommander par la commission de protection des droits de mettre en œuvre un moyen de sécurisation de son accès permettant de prévenir le renouvellement d'une utilisation de celui-ci à des fins de reproduction, de représentation ou de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits [...] lorsqu'elle est requise ;

2° Dans l'année suivant la présentation de cette recommandation, cet accès est à nouveau utilisé aux fins mentionnées au 1° du présent II. »

19. L'article L. 336 3 de ce code énonce :

« La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires [...] lorsqu'elle est requise.

Le manquement de la personne titulaire de l'accès à l'obligation définie au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé [...] »

2. Le décret du 5 mars 2010

20. Le décret du 5 mars 2010, dans sa version applicable aux faits du litige au principal, prévoit, à son article 1 :

« Le traitement de données à caractère personnel dénommé "Système de gestion des mesures pour la protection des œuvres sur l'internet" a pour finalité la mise en œuvre, par la commission de protection des droits de la [Hadopi] :

1° Des mesures prévues par le livre III de la partie législative du [CPI] (titre III, chapitre I^{er}, section 3, sous-section 3) et le livre III de la partie réglementaire du même code (titre III, chapitre I^{er}, section 2, sous-section 2) ;

2° Des saisines du procureur de la République de faits susceptibles de constituer des infractions prévues aux articles L. 335 2, L. 335 3, L. 335 4 et R. 335 5 du même code ainsi que de l'information des organismes de défense professionnelle et des organismes de gestion collective de ces saisines ;

[...] »

21. L'article 4 de ce décret dispose :

« I.- Ont directement accès aux données à caractère personnel et aux informations mentionnées à l'annexe au présent décret les agents publics assermentés habilités par le président de la [Hadopi] en application de l'article L. 331 21 du [CPI] et les membres de la commission de protection des droits mentionnée à l'article 1er.

II.- Les opérateurs de communications électroniques et les prestataires mentionnés au 2° de l'annexe au présent décret sont destinataires :

– des données techniques nécessaires à l'identification de l'abonné ;

– des recommandations prévues à l'article L. 331 25 du [CPI] en vue de leur envoi par voie électronique à leurs abonnés ;

– des éléments nécessaires à la mise en œuvre des peines complémentaires de suspension de l'accès à un service de communication au public en ligne portées à la connaissance de la commission de protection des

droits par le procureur de la République.

III.- Les organismes de défense professionnelle et les organismes de gestion collective sont destinataires d'une information relative à la saisine du procureur de la République.

IV.- Les autorités judiciaires sont destinataires des procès-verbaux de constatation de faits susceptibles de constituer des infractions prévues aux articles L. 335 2, L. 335 3, L. 335 4, L. 335 7, R. 331 37, R. 331 38 et R. 335 5 du [CPI].

Le casier judiciaire automatisé est informé de l'exécution de la peine de suspension. »

22. L'annexe au décret du 5 mars 2010 prévoit :

« Les données à caractère personnel et informations enregistrées dans le traitement dénommé « Système de gestion des mesures pour la protection des œuvres sur Internet » sont les suivantes :

1° Données à caractère personnel et informations provenant des organismes de défense professionnelle régulièrement constitués, des organismes de gestion collective, du Centre national du cinéma et de l'image animée ainsi que celles provenant du procureur de la République :

Quant aux faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336 3 du [CPI] :

Date et heure des faits ;

Adresse IP des abonnés concernés ;

Protocole pair à pair utilisé ;

Pseudonyme utilisé par l'abonné ;

Informations relatives aux œuvres ou objets protégés concernés par les faits ;

Nom du fichier tel que présent sur le poste de l'abonné (le cas échéant) ;

Fournisseur d'accès à Internet auprès duquel l'accès a été souscrit ou ayant fourni la ressource technique IP.

[...]

2° Données à caractère personnel et informations relatives à l'abonné recueillies auprès des opérateurs de communications électroniques [...] et des prestataires [...] :

Nom de famille, prénoms ;

Adresse postale et adresses électroniques ;

Coordonnées téléphoniques ;

Adresse de l'installation téléphonique de l'abonné ;

Fournisseur d'accès à Internet, utilisant les ressources techniques du fournisseur d'accès mentionné au 1°, auprès duquel l'abonné a souscrit son contrat ; numéro de dossier ;

date du début de la suspension de l'accès à un service de communication au public en ligne.

[...] »

3. Le code des postes et des télécommunications

23. L'article L. 34 1 du code des postes et des communications électroniques, tel que modifié par l'article 17 de la loi n° 2021 998 du 30 juillet 2021 (5) (ci-après le « CPCE »), dispose, à son paragraphe II bis, que « les opérateurs de communications électroniques sont tenus de conserver :

1° Pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale, les informations relatives à l'identité civile de l'utilisateur, jusqu'à l'expiration d'un délai de cinq ans à compter de la fin de validité de son contrat ;

2° Pour les mêmes finalités que celles énoncées au 1° du présent II bis, les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte ainsi que les informations relatives au paiement jusqu'à l'expiration d'un délai d'un an à compter de la fin de validité de son contrat ou de la clôture de son compte ;

3° Pour les besoins de la lutte contre la criminalité et la délinquance graves, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de de la sécurité nationale, les données techniques permettant d'identifier la source de connexion ou celles relatives aux équipements terminaux utilisés, jusqu'à l'expiration d'un délai d'un an à compter de la connexion ou de l'utilisation des équipements terminaux. »

III. Le litige au principal, les questions préjudicielles et la procédure devant la Cour

24. Par requête du 12 août 2019 et deux mémoires complémentaires du 12 novembre 2019 et du 6 mai 2021, La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, le Franciliens.net et le French Data Network ont introduit devant le Conseil d'État (France) une demande tendant à l'annulation de la décision implicite par laquelle le Premier ministre a rejeté leur demande visant l'abrogation du décret du 5 mars 2010, alors que ce décret et les dispositions constituant sa base légale non seulement porteraient une atteinte excessive aux droits garantis par la Constitution française, mais seraient également contraires à l'article 15 de la directive 2002/58 ainsi qu'aux articles 7, 8, 11, et 52 de la Charte.

25. En particulier, les requérants au principal font valoir que le décret du 5 mars 2010 et les dispositions qui en constituent la base légale autorisent l'accès à des données de connexion de façon disproportionnée pour des infractions relatives au droit d'auteur commises sur Internet et dépourvues de gravité, sans contrôle préalable d'un juge ou d'une autorité présentant des garanties d'indépendance et d'impartialité.

26. À cet égard, la juridiction de renvoi souligne, tout d'abord, que la Cour, dans son dernier arrêt La Quadrature du Net e.a. (6), a jugé que 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, ne s'oppose pas à des mesures législatives prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée *des données relatives à l'identité civile* des utilisateurs de moyens de communications électroniques. Ainsi, une telle conservation de ces données serait possible, sans délai particulier, aux fins de recherche, de détection et de poursuite des infractions pénales en général.

27. La juridiction de renvoi en déduit que le moyen soulevé par les requérants au principal relatif à l'illégalité du décret du 5 mars 2010, en ce qu'il a été adopté dans le cadre de la lutte contre des infractions dépourvues de gravité, ne peut être qu'écarté.

28. Cette juridiction rappelle, ensuite, que la Cour, dans son arrêt Tele2 Sverige et Watson (7), a jugé que 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, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante.

29. Elle relève que la Cour, dans l'arrêt Tele2 (8), a précisé que, aux fins de garantir, en pratique, le plein respect de ces conditions, il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, subordonné à l'exigence d'un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne 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.

30. La juridiction de renvoi souligne que la Cour a rappelé cette exigence dans l'arrêt La Quadrature du Net e.a. (9), s'agissant du recueil en temps réel des données de connexion par les services de renseignement, ainsi que dans l'arrêt Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (10), s'agissant de l'accès des autorités nationales aux données de connexion.

31. Cette juridiction observe, enfin, que, depuis sa création en 2009, la Hadopi a adressé plus de 12,7 millions de recommandations à des titulaires d'abonnements au titre de la procédure de réponse graduée prévue à l'article L 331 25 du CPI, dont 827 791 au cours de la seule année 2019. Pour ce faire, les agents de la commission de protection des droits de la Hadopi doivent pouvoir recueillir, chaque année, un nombre considérable de données relatives à l'identité civile des utilisateurs concernés. Elle estime que, compte tenu du volume de ces recommandations, le fait de soumettre ce recueil à un contrôle préalable risque de rendre impossible la mise en œuvre des recommandations.

32. C'est dans ces conditions que le Conseil d'État a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) Les données d'identité civile correspondant à une adresse IP sont-elles au nombre des données relatives au trafic ou de localisation soumises, en principe, à l'obligation d'un contrôle préalable par une juridiction ou une entité administrative indépendante dotée d'un pouvoir contraignant ?

2) S'il est répondu par l'affirmative à la première question, et eu égard à la faible sensibilité des données relatives à l'identité civile des utilisateurs, y compris leurs coordonnées, la directive [2002/58], lue à la lumière de la [Charte], doit-elle être interprétée comme s'opposant à une réglementation nationale prévoyant le recueil de ces données correspondant à l'adresse IP des utilisateurs par une autorité administrative, sans contrôle préalable par une juridiction ou une entité administrative indépendante dotée d'un pouvoir contraignant ?

3) S'il est répondu par l'affirmative à la deuxième question, et eu égard à la faible sensibilité des données relatives à l'identité civile, à la circonstance que seules ces données peuvent être recueillies, pour les seuls besoins de la prévention de manquements à des obligations définies de façon précise, limitative et restrictive par le droit national, et à la circonstance qu'un contrôle systématique de l'accès aux données de chaque utilisateur par une juridiction ou une entité administrative tierce dotée d'un pouvoir contraignant serait de nature à compromettre l'accomplissement de la mission de service public confiée à l'autorité administrative elle même indépendante qui procède à ce recueil, la directive [2002/58] fait-elle obstacle à ce que ce contrôle soit effectué selon des modalités adaptées, tel qu'un contrôle automatisé, le cas échéant sous la supervision d'un service interne à l'organisme présentant des garanties d'indépendance et d'impartialité à l'égard des agents chargés de procéder à ce recueil ? »

33. Les requérants au principal, les gouvernements français, estonien, suédois et norvégien ainsi que la Commission européenne ont présenté des observations écrites. Ces mêmes parties, à l'exception du gouvernement estonien, ainsi que les gouvernements danois et finlandais, ont été représentés à l'audience qui s'est tenue le 5 juillet 2022.

IV. Analyse

A. Sur les première et deuxième questions préjudicielles

34. Par ses première et deuxième questions préjudicielles, qu'il convient, selon moi, d'examiner ensemble, la juridiction de renvoi cherche à savoir, en substance, si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant l'accès, par une autorité administrative chargée de la protection des droits d'auteur et des droits voisins contre des atteintes à ces droits commises sur l'internet, à des données d'identité civile correspondant à des adresses IP afin que cette autorité puisse identifier les titulaires de ces adresses soupçonnés d'être responsables de ces atteintes et puisse prendre, le cas échéant, des mesures à leur égard, sans que cet accès soit subordonné à un contrôle préalable par une juridiction ou une entité administrative indépendante.

1. La délimitation des questions préjudicielles

a) La collecte préalable par les organismes d'ayants droit des adresses IP

35. Il ressort de la décision de renvoi que le mécanisme de réponse graduée en cause au principal comporte deux traitements de données successifs consistant, le premier, en la collecte préalable par les organismes d'ayants droit des adresses IP sur les réseaux de pair à pair de contrevenants au droit d'auteur et, le second, en la mise en relation de ces adresses IP avec l'identité civile des personnes par la Hadopi à la suite de sa saisine, aux fins de l'envoi de recommandation aux personnes dont l'accès à des services de communication au public en ligne a été utilisé en violation des règles relatives au droit d'auteur.

36. Les première et deuxième questions préjudicielles visent uniquement le second traitement réalisé par la Hadopi.

37. Les requérants au principal soutiennent toutefois que le premier traitement devrait faire l'objet d'un examen par la Cour, dans la mesure où, si ces adresses IP étaient obtenues en violation des dispositions de la directive 2002/58, leur exploitation dans le cadre du second traitement serait nécessairement contraire à ces dispositions.

38. Un tel raisonnement ne saurait convaincre. L'article 3, paragraphe 1, de la directive 2002/58 limite son champ d'application au « traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques ». Or, ainsi que l'a précisé le gouvernement français lors de l'audience, les organismes d'ayants droit obtiennent les adresses IP en cause non pas au moyen des fournisseurs de services de communications électroniques, mais directement en ligne, par la consultation de données disponibles pour le grand public.

39. Il peut donc seulement être constaté que la collecte préalable des adresses IP par les organismes d'ayants droit échappe aux dispositions de la directive 2002/58 et, ainsi que le relève la Commission, pourrait dès lors être analysée à la lumière des dispositions du règlement (UE) 2016/679 (11). Une telle analyse me semble ainsi excéder le cadre des questions préjudicielles posées à la Cour, et ce d'autant plus que la juridiction de renvoi n'apporte pas de précisions relatives à la collecte préalable qui permettrait à la Cour de lui fournir une réponse utile.

40. Dans ces conditions, je concentrerai mon analyse sur la question de l'accès, par la Hadopi, aux données d'identité civile correspondant à une adresse IP.

b) Le couplage des adresses IP et des données d'identité civile

41. Les première et deuxième questions préjudicielles visent « les données d'identité civile correspondant à une adresse IP », qui seraient, selon la juridiction de renvoi, d'une faible sensibilité. Cette juridiction se réfère exclusivement, dans sa décision, aux points de l'arrêt Quadrature du Net e.a. relatifs à la conservation des données d'identité civile.

42. Il est vrai que la jurisprudence de la Cour effectue une distinction entre le régime de conservation et d'accès des adresses IP et le régime de conservation et d'accès des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, ce second régime étant moins strict que le premier (12).

43. Cependant, il me semble que, en l'espèce, malgré la formulation de ces deux questions préjudicielles, est non pas en cause la question du seul accès aux données d'identité civile des utilisateurs de moyens de communications électroniques, mais bien la mise en relation de ces données aux adresses IP dont dispose la Hadopi à la suite du recueil et de la transmission de ces dernières par les organismes d'ayants droit. En effet, ainsi que le relève la Commission, l'accès aux données d'identité civile par la Hadopi vise à débloquer un ensemble plus large de données, notamment les adresses IP et les extraits de fichiers consultés, et à permettre leur exploitation, les données d'identité civile et les adresses IP étant, indépendamment les unes des autres, sans intérêt pour les autorités nationales dès lors que ni l'identité civile ni l'adresse IP en soi ne peuvent donner d'informations sur les activités des personnes physiques en ligne lorsqu'elles ne sont pas mises en relation.

44. Il s'ensuit qu'il convient, à mon sens, de comprendre les première et deuxième questions préjudicielles comme visant non seulement les données d'identité civile des utilisateurs d'un moyen de communication électronique mais également l'accès aux adresses IP permettant d'identifier la source d'une connexion.

c) La conservation des adresses IP par les fournisseurs de services de communication

45. Il est vrai, ainsi que le relèvent le gouvernement français et la Commission, que les questions préjudicielles posées à la Cour visent non pas, formellement, la conservation des données par les fournisseurs de services de communications électroniques, mais le seul accès, par la Hadopi, à des données d'identité civile correspondant à des adresses IP.

46. Toutefois, la question de l'accès par la Hadopi à ces données me semble en réalité indissociable de celle, préalable, de leur conservation par les fournisseurs de services de communications. Ainsi que l'a souligné la Cour, la conservation de données n'intervient qu'aux seules fins de rendre, le cas échéant, les données accessibles aux autorités nationales compétentes (13). Autrement dit, la conservation et l'accès à des données ne sauraient se concevoir isolément, alors même que le second est dépendant de la première.

47. Certes, la Cour a déjà examiné la compatibilité avec l'article 15, paragraphe 1, de la directive 2002/58 d'une réglementation nationale relative au seul accès par les autorités nationales compétentes à certaines données à caractère personnel indépendamment de la question de la compatibilité avec cette disposition de la conservation des données en cause (14). Il pourrait dès lors être répondu aux présentes questions préjudicielles en faisant abstraction du point de savoir si les données en cause ont été conservées conformément aux dispositions du droit de l'Union.

48. Cependant, je relève, tout d'abord, que, dans l'arrêt Ministerio Fiscal (15), l'examen mené par la Cour s'agissant de la compatibilité avec le droit de l'Union de l'accès des autorités nationales à certaines données personnelles répond strictement aux mêmes principes que celui qu'elle mène s'agissant d'évaluer la compatibilité

avec le droit de l'Union de la conservation de ces données. En effet, la Cour se réfère exclusivement à la jurisprudence développée à ce dernier égard afin de la transposer à la question de l'accès à des données à caractère personnel. Autrement dit, en l'absence d'examen de la compatibilité avec le droit de l'Union de la conservation de certaines données, cet examen est reporté au stade de la question de l'accès à ces données, de sorte que la compatibilité de cet accès dépend in fine de celle de la conservation.

49. Ensuite, la Cour a clairement indiqué que l'accès à des données à caractère personnel ne peut être octroyé que pour autant que ces données aient été conservées par les fournisseurs de services de communications électroniques d'une manière conforme à l'article 15, paragraphe 1, de la directive 2002/58 (16) et que l'accès à des données à caractère personnel par des personnes privées pour permettre d'engager, devant des juridictions civiles, des poursuites contre les atteintes au droit d'auteur n'est compatible avec le droit de l'Union qu'à la condition que ces données soient conservées de manière compatible avec cette disposition (17).

50. Enfin, la Cour juge de façon constante que l'accès à des données relatives au trafic et à des données de localisation conservées par des fournisseurs en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58, qui doit s'effectuer dans le plein respect des conditions résultant de la jurisprudence ayant interprété la directive 2002/58, ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs (18). En d'autres termes, la compatibilité avec le droit de l'Union de l'accès par les autorités nationales à certaines données à caractère personnel est entièrement dépendante de la compatibilité avec le droit de l'Union de la conservation de ces données.

51. Il en résulte, à mon sens, que l'analyse de la compatibilité avec le droit de l'Union d'une réglementation nationale prévoyant l'accès par une autorité nationale à des données à caractère personnel suppose d'avoir établi, au préalable, la compatibilité avec le droit de l'Union de la conservation de ces mêmes données.

52. Dans ces conditions, je débuterai mon analyse par un rappel de la jurisprudence de la Cour relative à la question de la conservation des adresses IP attribuées à la source d'une connexion, afin d'en démontrer les limites, et de proposer une grille de lecture aménagée de la réglementation en cause.

2. La jurisprudence de la Cour relative à l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 s'agissant de mesures visant la conservation des adresses IP attribuées à la source d'une connexion

53. L'article 5, paragraphe 1, de la directive 2002/58 consacre le principe de confidentialité tant des communications électroniques que des données relatives au trafic y afférentes et implique, notamment, l'interdiction faite, en principe, à toute personne autre que les utilisateurs de stocker, sans le consentement de ceux-ci, ces communications et ces données (19).

54. S'agissant du traitement et du stockage par les fournisseurs de services de communications électroniques des données relatives au trafic concernant les abonnés et les utilisateurs, la directive 2002/58 prévoit, à son article 6, paragraphe 1, que ces données doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication et précise, à son article 6, paragraphe 2, que les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion ne peuvent être traitées que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement. Quant aux données de localisation autres que les données relatives au trafic, l'article 9, paragraphe 1, de cette directive énonce que ces données ne peuvent être traitées que sous certaines conditions et après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés (20).

55. Ainsi, en adoptant la directive 2002/58, le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte, de telle sorte que les utilisateurs de moyens de communication électronique sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement (21). Partant, cette directive ne se limite pas à encadrer l'accès à de telles données par des garanties visant à prévenir les abus, mais consacre aussi, en particulier, le principe de l'interdiction de leur stockage par des tiers.

56. Dans ces conditions, en ce que 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, notamment, aux articles 5, 6 et 9 de cette directive, tels que ceux découlant des principes de confidentialité des communications et de l'interdiction du stockage des données y afférentes, cette disposition énonce une exception à la règle générale prévue, notamment, à ces articles 5, 6 et 9 et doit ainsi, conformément à une jurisprudence constante, faire l'objet d'une interprétation stricte. Une telle disposition ne saurait donc justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y

afférentes et, en particulier, à l'interdiction de stocker ces données, prévue à l'article 5 de ladite directive, devienne la règle, sauf à vider cette dernière disposition de sa portée (22).

57. Quant aux objectifs susceptibles de justifier une limitation des droits et des obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58, la Cour a déjà jugé que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de cette directive revêt un caractère exhaustif, de telle sorte qu'une mesure législative adoptée au titre de cette disposition doit répondre effectivement et strictement à l'un de ces objectifs (23).

58. En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 que les mesures prises par les États membres au titre de cette disposition doivent respecter les principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et assurer le respect des droits fondamentaux garantis par la Charte. À cet égard, la Cour a déjà jugé que l'obligation imposée par un État membre aux fournisseurs de services de communications électroniques, par une législation nationale, de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, relatifs, respectivement à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel, mais également de l'article 11 de la Charte, relatif à la liberté d'expression, cette liberté constituant l'un des fondements essentiels d'une société démocratique et pluraliste, et faisant partie des valeurs sur lesquelles, conformément à l'article 2 TUE, est fondée l'Union (24).

59. Cela étant, en ce que l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres de limiter les droits et les obligations prévus aux articles 5, 6, et 9 de cette directive, cette disposition reflète la circonstance que les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais comme devant être pris en considération par rapport à leur fonction dans la société. En effet, ainsi qu'il ressort de son article 52, paragraphe 1, la Charte admet des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui. Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de la Charte, requiert de tenir compte également de l'importance que revêtent les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave en contribuant à la protection des droits et des libertés d'autrui et de celle des droits consacrés aux articles 3, 4, 6 et 7 de la Charte (25), dont sont susceptibles de découler des obligations positives à la charge des pouvoirs publics (26).

60. Face à ces différentes obligations positives, il convient donc de procéder à une conciliation des différents intérêts légitimes et des droits en cause. Dans ce cadre, il découle des termes mêmes de l'article 15, paragraphe 1, première phrase, de la directive 2002/58 que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité lorsqu'une telle mesure est « nécessaire, appropriée et proportionnée, au sein d'une société démocratique », le considérant 11 de cette directive indiquant, à cet effet, qu'une mesure de cette nature doit être « rigoureusement » proportionnée au but poursuivi (27).

61. À cet égard, il découle de la jurisprudence de la Cour que la possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58 doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité (28).

62. Je relève, en outre, que la Cour distingue, dans sa jurisprudence, d'une part, les ingérences résultant de l'accès à des données qui, en tant que telles, fournissent des informations précises sur les communications en cause et, donc, sur la vie privée de la personne, et pour lesquelles le régime de conservation est strict, et, d'autre part, les ingérences qui résultent de l'accès à des données, qui ne peuvent fournir de telles informations qu'en tant qu'elles sont couplées à d'autres données, telles que les adresses IP (29).

63. S'agissant plus particulièrement des adresses IP, la Cour a ainsi relevé qu'elles sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'internet est effectuée. Dès lors, pour autant que seules les adresses IP de la source de la communication sont conservées et non celles du destinataire de celle-ci, cette catégorie de données présente un degré de sensibilité moindre que les autres données relatives au trafic (30).

64. La Cour souligne dans le même temps que, dès lors que les adresses IP peuvent être utilisées pour effectuer, notamment, un traçage exhaustif du parcours de navigation d'un internaute et, par la suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier et de tirer des conclusions précises sur la vie privée de l'utilisateur. La conservation et l'analyse de ces adresses IP constituent donc des ingérences *graves* dans les

droits fondamentaux consacrés aux articles 7 et 8 de la Charte, et peuvent avoir des effets dissuasifs sur l'exercice de la liberté d'expression garantie à l'article 11 de celle-ci (31).

65. Toutefois, selon une jurisprudence constante, il y a lieu, aux fins de la conciliation nécessaire des droits et des intérêts légitimes en cause exigée par la jurisprudence, de tenir compte du fait que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction (32).

66. Partant, la Cour juge qu'une mesure législative prévoyant la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion n'apparaît pas, en principe, contraire à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, cette possibilité devant être soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données et étant entendu que, eu égard au caractère grave de l'ingérence que comportent cette conservation, seule la lutte contre la *criminalité grave* et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sécurité nationale, à justifier cette ingérence (33).

67. La Cour précise en outre que la durée de la conservation ne saurait excéder celle qui est strictement nécessaire au regard de l'objectif poursuivi et qu'une mesure de cette nature doit prévoir des conditions et des garanties strictes quant à l'exploitation de ces données (34).

3. Les limites de la jurisprudence relative à l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 s'agissant de mesures visant la conservation des adresses IP attribuées à la source d'une connexion

68. La solution à laquelle est parvenue la Cour s'agissant de mesures nationales visant la conservation des adresses IP attribuées à la source d'une connexion, interprétées à la lumière de l'article 15, paragraphe 1, de la directive 2002/58, me semble cependant présenter deux difficultés principales.

a) La conciliation avec la jurisprudence relative à la communication des adresses IP attribuées à la source d'une connexion dans le cadre des recours en protection des droits de propriété intellectuelle

69. En premier lieu, ainsi que je l'avais déjà évoqué dans mes conclusions dans l'affaire M.I.C.M. (35), il existe une tension certaine entre cette ligne de jurisprudence et celle relative à la communication des adresses IP dans le cadre des recours en protection des droits de propriété intellectuelle aux titulaires de ces droits, qui met l'accent sur l'obligation des États membres d'assurer aux titulaires des droits de propriété intellectuelle des possibilités réelles d'obtenir une réparation des préjudices résultant des atteintes à ces droits (36).

70. En effet, en ce qui concerne cette seconde ligne de jurisprudence, la Cour juge de façon constante que le droit de l'Union ne s'oppose pas à ce que les États membres établissent une obligation de transmission à des personnes privées de données à caractère personnel pour permettre d'engager, devant les juridictions civiles, des poursuites contre les atteintes au droit d'auteur (37).

71. La Cour relève, à cet égard, que la possibilité, pour les États membres, de prévoir l'obligation de divulguer, dans le cadre de poursuites civiles, des données à caractère personnel découle d'abord de la possibilité de prévoir une telle divulgation dans le cadre de la poursuite d'infractions pénales (38), qui a par la suite été élargie aux poursuites civiles.

72. Dans le même temps, s'agissant des adresses IP, la Cour impose cependant que ces données ne peuvent être conservées que dans le cadre de la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique (39).

73. Les tentatives de réconciliation de ces deux lignes de jurisprudence conduisent, selon moi, à des résultats inadaptés et ne sauraient convaincre.

74. D'une part, contrairement à ce qu'a soutenu le gouvernement français lors de l'audience, la lutte contre les violations des droits de propriété intellectuelle ne saurait relever de la lutte contre la criminalité grave. La notion de « criminalité grave » doit, à mon sens, recevoir une interprétation autonome. Elle ne saurait dépendre des conceptions de chaque État membre sauf à permettre un contournement des exigences de l'article 15, paragraphe 1, de la directive 2002/58 selon que les États membres adoptent une conception extensive ou non de la lutte contre la criminalité grave. Or, ainsi que je l'ai déjà relevé, les intérêts liés à la protection des droits de propriété intellectuelle ne sauraient se confondre avec ceux qui sous-tendent la lutte contre la criminalité grave (40).

75. D'autre part, admettre la transmission d'adresses IP aux titulaires de droits de propriété intellectuelle dans le cadre des procédures ayant pour objet leur protection, alors même que leur conservation n'est rendue possible

que dans le cadre de la lutte contre la criminalité grave, irait clairement à l'encontre de la jurisprudence de la Cour relative à la conservation des données de connexion et reviendrait à priver d'effet utile les conditions requises pour la conservation de telles données, dès lors qu'il pourrait en tout état de cause y être accédé pour des motifs différents.

76. Il en résulte, selon moi, que la conservation des adresses IP aux fins de la protection des droits de propriété intellectuelle ainsi que leur communication aux titulaires de ces droits dans le cadre des procédures ayant pour objet cette protection pourraient être contraires à l'article 15, paragraphe 1, de la directive 2002/58, tel qu'interprété dans la jurisprudence de la Cour. L'obligation de transmission à des personnes privées de données à caractère personnel pour permettre d'engager, devant les juridictions civiles, des poursuites contre les atteintes au droit d'auteur, pourtant rendue possible par la Cour elle-même, est donc dans le même temps neutralisée par le jeu de sa propre jurisprudence relative à la conservation des adresses IP par les fournisseurs de services de communications électroniques.

77. Une telle solution n'est toutefois pas satisfaisante en ce qu'elle remettrait en cause l'équilibre des différents intérêts en jeu que la Cour a cherché à établir, en privant les titulaires de droits de propriété intellectuelle du principal, sinon seul, moyen d'identifier les auteurs des atteintes à ces droits en ligne. Cette considération m'amène à exposer la seconde difficulté qui peut résulter, à mes yeux, de la jurisprudence de la Cour, s'agissant de mesures nationales visant la conservation des adresses IP attribuées à la source d'une connexion interprétée à la lumière de l'article 15, paragraphe 1, de la directive 2002/58.

b) Le risque d'une impunité systémique pour les infractions constituées exclusivement en ligne

78. Ainsi, en second lieu, je suis d'avis que cette solution est la source de difficultés pratiques. Ainsi que le souligne la Cour elle-même, dans le cas d'une infraction commise exclusivement en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction.

79. Pour autant, il me semble que cet élément n'est pas entièrement pris en compte dans la mise en balance des intérêts en cause. Dès lors que la Cour limite tout de même la possibilité de conservation des adresses IP au cadre de la lutte contre la criminalité grave, elle exclut dans le même temps que ces données puissent être conservées afin de lutter contre des infractions pénales en général, alors que certaines de ces infractions ne peuvent être prévenues, détectées ou sanctionnées que grâce auxdites données.

80. En d'autres termes, la jurisprudence de la Cour pourrait conduire à priver les autorités nationales du seul moyen d'identification des auteurs d'infractions en ligne ne relevant toutefois pas de la criminalité grave, telles que les infractions aux droits de propriété intellectuelle. Il en résulterait de fait une impunité systémique pour les infractions commises exclusivement en ligne, au-delà d'ailleurs des seules infractions aux droits de propriété intellectuelle. Je songe notamment aux actes de diffamation commis en ligne. Le droit de l'Union prévoit certes des injonctions à l'encontre des intermédiaires dont les services sont utilisés pour la commission de telles infractions (41), mais il pourrait résulter de la jurisprudence de la Cour que les auteurs mêmes de ces actes pourraient n'être jamais poursuivis.

81. Sauf à admettre que toute une série d'infractions pénales ne puisse jamais faire l'objet de poursuites, je suis d'avis que l'équilibre entre les différents intérêts en présence devrait faire l'objet d'une nouvelle analyse.

82. Ces différentes considérations me conduisent à proposer à la Cour un certain aménagement de la jurisprudence relative aux mesures nationales visant la conservation des adresses IP interprétées à la lumière de l'article 15, paragraphe 1, de la directive 2002/58.

4. La proposition d'un aménagement de la jurisprudence de la Cour relative à l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 s'agissant de mesures visant la conservation des adresses IP attribuées à la source d'une connexion

83. Compte tenu des considérations qui précèdent, je suis d'avis que l'article 15, paragraphe 1, de la directive 2002/58 devrait être interprété comme ne s'opposant pas à des mesures prévoyant une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire, aux fins d'assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales en ligne pour lesquelles l'adresse IP constitue *le seul moyen* d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de l'infraction.

84. Il me faut souligner, à cet égard, qu'une telle proposition ne remet pas en cause, à mon sens, l'exigence de proportionnalité imposée pour la conservation des données, eu égard au caractère grave de l'ingérence dans les

droits fondamentaux consacrés aux articles 7 et 8 de la Charte que cette ingérence implique (42). Au contraire, elle satisfait pleinement à cette exigence.

85. D'une part, la limitation aux droits et obligations prévus aux articles 5, 6 et 9 de la directive 2002/58 que constitue la conservation des adresses IP poursuit un objectif d'intérêt général en relation avec cette gravité, à savoir la prévention, la recherche, la détection et la poursuite d'infractions pénales visées par des textes qui resteraient autrement dépourvus d'effet.

86. D'autre part, cette limitation s'opère dans les limites du strict nécessaire. En effet, une telle conservation est limitée à des hypothèses précises, à savoir les infractions pénales commises en ligne et pour lesquelles l'identification de son auteur ne peut avoir lieu que grâce à l'adresse IP qui lui est attribuée. Autrement dit, il s'agit non pas d'autoriser une conservation généralisée et indifférenciée des données sans autres conditions, mais seulement de permettre la poursuite d'infractions pénales non pas en règle générale, mais bien déterminées.

87. Toutefois, si l'article 15, paragraphe 1, de la directive 2002/58 ne s'oppose pas à une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion aux fins d'assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales en ligne pour lesquelles l'adresse IP constitue le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de l'infraction, il faut encore préciser que, selon la jurisprudence, cette possibilité doit être soumise « au strict respect des conditions matérielles et procédurales *devant régir l'utilisation de ces données* » (43). La Cour précise également qu'une telle mesure « doit prévoir des conditions et des garanties strictes quant à *l'exploitation de ces données* » (44).

88. Autrement dit, ainsi que je l'ai déjà souligné, la conservation des données et l'accès à ces données ne sauraient se concevoir isolément. Dans ces conditions, si la possibilité pour la Hadopi d'accéder aux adresses IP n'est pas d'emblée contraire à l'article 15, paragraphe 1, de la directive 2002/58 dans la mesure où ces données ont été conservées en conformité avec les exigences prévues à cette disposition, il est encore nécessaire, afin de répondre aux questions préjudicielles soumises à la Cour, d'examiner si les conditions d'accès aux adresses IP attribuées à la source d'une connexion par la Hadopi sont, en elles-mêmes, conformes à ladite disposition, en particulier s'agissant de la nécessité ou non d'un contrôle préalable d'un tel accès par une juridiction ou une autorité administrative indépendante.

89. Ayant analysé la question préliminaire de la conservation des adresses IP attribuées à la source d'une connexion, je procéderai à l'examen de l'accès à ces données par la Hadopi à la lumière de l'article 15, paragraphe 1, de la directive 2002/58.

5. L'accès aux données d'identité civile correspondant aux adresses IP par la Hadopi

90. Il ressort de la jurisprudence de la Cour, s'agissant des objectifs susceptibles de justifier une mesure nationale dérogeant au principe de confidentialité des communications électroniques, que l'accès aux données doit répondre strictement et objectivement à l'un de ces objectifs, et que l'objectif poursuivi par cette mesure doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux qu'entraîne cet accès (45).

91. En outre, ainsi que je l'ai exposé (46), l'accès à des données conservées par des fournisseurs en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58 ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs (47).

92. La Cour a ainsi jugé, conformément au principe de proportionnalité, qu'une ingérence grave ne peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, que par un objectif de lutte contre la criminalité devant également être qualifiée de grave (48).

93. À cet égard, je relève, contrairement à ce que soutiennent le gouvernement français et la Commission, que l'accès par la Hadopi aux données d'identité civile correspondant à une adresse IP constitue bien une ingérence grave dans les droits fondamentaux. En effet, il ne s'agit pas seulement d'accéder aux données d'identité civile, qui sont, en elles-mêmes, d'une faible sensibilité, mais bien de mettre en relation ces données à un ensemble plus large de données, à savoir l'adresse IP, et également, comme le soulignent les requérants au principal, un extrait du fichier téléchargé en violation du droit d'auteur. Il est donc question de lier l'identité civile d'une personne au contenu du fichier consulté et à l'adresse IP par laquelle a eu lieu cette consultation.

94. Cependant, de la même façon que je suis d'avis de permettre également la conservation de données constituant une ingérence grave aux droits fondamentaux aux fins d'assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales en ligne pour lesquelles l'adresse IP constitue le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de l'infraction (49), je crois que l'accès à ces données devrait être rendu possible afin de poursuivre le même objectif, sauf à admettre l'impunité générale des infractions exclusivement commises en ligne.

95. L'accès par la Hadopi aux données d'identité civile couplées à une adresse IP m'apparaît donc justifié par l'objectif d'intérêt général pour lequel cette conservation a été imposée aux fournisseurs de services de communications électroniques.

96. La jurisprudence de la Cour précise toutefois qu'une législation nationale régissant l'accès des autorités compétentes à des données relatives au trafic et à des données de localisation conservées ne saurait se limiter à exiger que l'accès réponde à la finalité poursuivie par cette législation, mais elle doit également prévoir les conditions matérielles et procédurales régissant l'accès des autorités nationales compétentes aux données concernées (50).

97. En particulier, la Cour juge que, dès lors qu'un accès général à toutes les données conservées, indépendamment d'un quelconque lien avec le but poursuivi, ne saurait être considéré comme limité au strict nécessaire, la réglementation nationale 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 utilisateurs, de sorte à vérifier que l'accès n'est accordé qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou d'être impliquées d'une manière ou d'une autre dans une telle infraction (51).

98. Ainsi, selon la jurisprudence, aux fins de garantir, en pratique, le plein respect de ces conditions, il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante (52).

99. Toutefois, je relève que la Cour a établi cette nécessité d'un contrôle préalable de l'accès aux données personnelles dans des circonstances particulières qui diffèrent de la présente espèce, impliquant des intrusions *particulièrement graves* et dans la vie privée des utilisateurs de services de communications électroniques.

100. En effet, il s'agissait, dans chacun des arrêts ayant souligné cette exigence, de mesures nationales autorisant l'accès à l'ensemble des données relatives au trafic et à la localisation des utilisateurs relatives à tous les moyens de communication électronique (53) ou, à tout le moins, à la téléphonie fixe et mobile (54). Plus précisément, était en cause l'accès à un « ensemble de données [...] susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée » (55), de sorte que l'exigence d'un contrôle préalable de l'accès à ces données par une juridiction ou une entité administrative indépendante n'existe, à mon sens, que dans ces conditions.

101. Or, d'une part, l'accès par la Hadopi reste limité à mettre en relation les données d'identité civile à l'adresse IP utilisée et au fichier consulté à un moment précis, sans que cela conduise à permettre aux autorités compétentes de reconstruire le parcours de navigation en ligne de l'utilisateur visé, ni, dès lors, de tirer des conclusions précises sur sa vie privée au-delà de la connaissance du fichier précis consulté au moment de l'infraction. Il ne s'agit donc pas de permettre le traçage de l'ensemble des activités en ligne de l'utilisateur en cause.

102. D'autre part, ces données ne concernent que les données de personnes qui, ainsi que cela a été constaté dans les procès-verbaux établis par les organismes d'ayants droit, se sont livrées à des faits susceptibles de constituer un manquement à l'obligation prévue à l'article L.336-3 du CPI. L'accès par la Hadopi aux données d'identité civile couplées aux adresses IP est donc strictement limité à ce qui est nécessaire pour atteindre l'objectif poursuivi, à savoir permettre la prévention, la recherche, la détection et la poursuite d'infractions pénales en ligne pour lesquelles l'adresse IP constitue le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de l'infraction, dans lequel s'inscrit le mécanisme de riposte graduée.

103. Dans ces conditions, je suis d'avis que l'article 15, paragraphe 1, de la directive 2002/58 n'impose pas l'existence d'un contrôle préalable de l'accès par la Hadopi aux données d'identité civile couplées aux adresses IP des utilisateurs par une juridiction ou une entité administrative indépendante.

104. Pour le surplus, je relève, ainsi que le souligne le gouvernement français, que l'accès par la Hadopi à ces données, s'il n'est pas soumis à un contrôle préalable par une juridiction ou une entité indépendante, n'est toutefois pas exempt de tout contrôle, dès lors que le fichier envoyé par la Hadopi aux opérateurs de communications électroniques est constitué chaque jour par un agent assermenté à partir des saisines reçues et validées, de manière aléatoire par échantillon, avant leur adjonction au fichier (56). Surtout, il convient d'observer que la procédure de réponse graduée demeure soumise aux dispositions de la directive (UE) 2016/680 (57). À ce titre, les personnes physiques visées par la Hadopi bénéficient d'un ensemble de garanties matérielles et procédurales prévues par cette directive. Celles-ci englobent le droit d'accès, de rectification et d'effacement des données personnelles traitées par la Hadopi, ainsi que la possibilité de procéder à une réclamation auprès d'une

autorité de contrôle indépendante, suivie, le cas échéant, d'un recours juridictionnel exercé dans les conditions de droit commun (58).

105. Partant, je propose de répondre aux première et deuxième questions préjudicielles que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale permettant la conservation par les fournisseurs de services de communications électroniques et l'accès par une autorité administrative chargée de la protection des droits d'auteur et des droits voisins contre des atteintes à ces droits commises sur l'internet limité à des données d'identité civile correspondant à des adresses IP afin que cette autorité puisse identifier les titulaires de ces adresses soupçonnés d'être responsables de ces atteintes et puisse prendre, le cas échéant, des mesures à leur égard, sans que cet accès soit subordonné à un contrôle préalable par une juridiction ou une entité administrative indépendante, lorsque ces données constituent le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de l'infraction.

B. Sur la troisième question préjudicielle

106. Par sa troisième question préjudicielle, la juridiction de renvoi cherche à savoir si, dans l'hypothèse où il était répondu par l'affirmative aux première et deuxième questions, et eu égard à la faible sensibilité des données d'identité civile, à l'encadrement strict de l'accès aux données et à l'impératif de ne pas compromettre la mission de service public confiée à l'autorité administrative en cause, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8, et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à ce que le contrôle préalable de l'accès soit effectué selon des modalités adaptées, tel qu'un contrôle automatisé, le cas échéant sous la supervision d'un service interne à l'organisme présentant des garanties d'indépendance et d'impartialité à l'égard des agents chargés de procéder à ce recueil.

107. Il ressort du libellé de la troisième question préjudicielle ainsi que de la réponse écrite du gouvernement français aux questions de la Cour que les modalités de contrôle adaptées auxquelles il est fait référence dans cette question visent non pas un dispositif de contrôle existant en droit national, mais les pistes pouvant être explorées et visant à mettre le dispositif français en conformité avec le droit de l'Union le cas échéant.

108. Or, il est de jurisprudence constante qu'une demande de décision préjudicielle n'a pas pour objectif la formulation d'opinions consultatives sur des questions générales et hypothétiques, mais vise à satisfaire le besoin inhérent à la solution effective d'un litige portant sur le droit de l'Union (59).

109. La troisième question préjudicielle revêtant donc, à mon sens, un caractère hypothétique, il y a lieu de la juger irrecevable.

110. En tout état de cause, compte tenu de la réponse que je propose d'apporter aux première et deuxième questions préjudicielles, il n'y a pas lieu de répondre à la troisième question.

V. Conclusion

111. Eu égard à l'ensemble des considérations qui précèdent, je propose à la Cour de répondre comme suit aux questions préjudicielles posées par le Conseil d'État (France) :

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 à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne

doit être interprété en ce sens que :

il ne s'oppose pas à une réglementation nationale permettant la conservation par les fournisseurs de services de communications électroniques et l'accès par une autorité administrative chargée de la protection des droits d'auteur et des droits voisins contre des atteintes à ces droits commises sur l'internet limité à des données d'identité civile correspondant à des adresses IP afin que cette autorité puisse identifier les titulaires de ces adresses soupçonnés d'être responsables de ces atteintes et puisse prendre, le cas échéant, des mesures à leur égard, sans que cet accès soit subordonné à un contrôle préalable par une juridiction ou une entité administrative indépendante, lorsque ces données constituent le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de l'infraction.

---

1 Langue originale : le français.

2 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).

3 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).

4 JORF du 7 mars 2010, texte n°°19.

5 JORF du 31 juillet 2021, texte n° 1. Cette version de l'article L. 34 1 du CPCE, en vigueur depuis le 31 juillet 2021, a été adoptée à la suite de la décision du Conseil d'État (France) du 21 avril 2021, n° 393099 (JORF du 25 avril 2021) ayant écarté la version précédente de cette disposition qui incluait une obligation de conservation de données à caractère personnel « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336 3 [du CPI] » dans le seul but de permettre, en tant que besoin, la mise à disposition, notamment, de la Hadopi. Par décision n° 2021-976-977 QPC, du 25 février 2022 (M. Habib A. et autre), le Conseil constitutionnel (France) a déclaré contraire à la Constitution cette précédente version de l'article L. 34 1 du CPCE au motif essentiel que, « en autorisant la conservation générale et indifférenciée des données de connexion, les dispositions contestées portent une atteinte disproportionnée au droit au respect de la vie privée » (point 13). Cette juridiction a en effet considéré que les données de connexion devant être conservées en vertu de ces dispositions portent non seulement sur l'identification des utilisateurs des services de communications électroniques mais aussi sur d'autres données qui, « compte tenu de leur nature, de leur diversité et des traitements dont elles peuvent faire l'objet [...] fournissent sur ces utilisateurs ainsi que, le cas échéant, sur des tiers, des informations nombreuses et précises, particulièrement attentatoires à leur vie privée » (point 11).

6 Voir arrêt du 6 octobre 2020 (C 511/18, C 512/18 et C 520/18, ci-après l'« arrêt La Quadrature du Net e.a. », EU:C:2020:791, dispositif).

7 Voir arrêt du 21 décembre 2016 (C 203/15 et C 698/15, ci-après l'« arrêt Tele2 », EU:C:2016:970, dispositif).

8 Point 120 de cet arrêt.

9 Point 189 de cet arrêt.

10 Arrêt du 2 mars 2021 (C 746/18, ci-après l'« arrêt Prokuratuur », EU:C:2021:152).

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

12 Voir arrêt Quadrature du Net e.a. (points 155 et 159).

13 Voir arrêt Tele2 (point 79).

14 Voir arrêt du 2 octobre 2018, Ministerio Fiscal (C 207/16, EU:C:2018:788, point 49).

15 Arrêt du 2 octobre 2018 (C 207/16, EU:C:2018:788).

16 Voir arrêt Prokuratuur (point 29).

17 Voir arrêt du 17 juin 2021, M.I.C.M. (C 597/19, EU:C:2021:492, points 127 à 130).

18 Voir arrêts La Quadrature du Net e.a., point 166) ; du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C 140/20, ci-après l'« arrêt Commissioner of An Garda Síochána e.a. », EU:C:2022:258, point 98), et du 20 septembre 2022, SpaceNet, (C 793/19 et C-794/19, ci-après l'« arrêt SpaceNet », EU:C:2022:702, point 131).

19 Voir arrêts La Quadrature du Net e.a. (point 107) ; Commissioner of An Garda Síochána e.a. (point 35), et SpaceNet (point 52).

20 Voir arrêts Tele2 (point 86) ; La Quadrature du Net e.a. (point 108) ; Commissioner of An Garda Síochána e.a. (point 38), et SpaceNet (point 55).

21 Voir arrêts La Quadrature du Net e.a. (point 109) ; Commissioner of An Garda Síochána e.a. (point 37), et SpaceNet (point 54).

22 Voir arrêts La Quadrature du Net e.a. (points 110 et 111) ; Commissioner of An Garda Síochána e.a. (point 40), et SpaceNet (point 57).

23 Voir arrêts La Quadrature du Net e.a. (point 112) ; Commissioner of An Garda Síochána e.a. (point 41), et SpaceNet (point 58).

24 Voir arrêts La Quadrature du Net e.a. (points 113 et 114) ; Commissioner of An Garda Síochána e.a. (point 42), et SpaceNet (point 60).

25 Voir arrêts La Quadrature du Net e.a. (points 120 à 122) ; Commissioner of An Garda Síochána e.a. (point 48), et SpaceNet (point 63).

26 Voir arrêts La Quadrature du Net e.a. (points 120 à 122) ; Commissioner of An Garda Síochána e.a. (point 49), et SpaceNet (point 64).

27 Voir arrêts La Quadrature du Net e.a. (points 127 à 129) ; Commissioner of An Garda Síochána e.a. (points 50 et 51), et SpaceNet (points 65 et 66).

28 Voir arrêts La Quadrature du Net e.a. (point 131) ; Commissioner of An Garda Síochána e.a. (point 53), et SpaceNet (point 68).

29 Voir points 41 et suiv. des présentes conclusions.

30 Voir arrêt La Quadrature du Net e.a. (point 152).

31 Voir arrêts La Quadrature du Net e.a. (point 153) ; Commissioner of An Garda Síochána e.a. (point 73), et SpaceNet (point 103) (italique ajouté par mes soins).

32 Voir arrêts La Quadrature du Net e.a. (point 154) ; Commissioner of An Garda Síochána e.a. (point 73), et SpaceNet (point 103).

33 Voir arrêts La Quadrature du Net e.a. (points 155 et 156) ; Commissioner of An Garda Síochána e.a. (point 74), et SpaceNet (points 104 et 105) (italique ajouté par mes soins).

34 Voir arrêts La Quadrature du Net e.a. (point 156) et SpaceNet (point 105).

35 C 597/19, EU:C:2020:1063, point 98.

36 Voir mes conclusions dans l'affaire M.I.C.M. (C 597/19, EU:C:2020:1063, point 97).

37 Voir arrêts du 19 avril 2012, Bonnier Audio e.a. (**C-461/10,** EU:C:2012:219, **point 55) ;** du 4 mai 2017, Rīgas satiksme (**C-13/16,** EU:C:2017:336, **point 34)**, et du 17 juin 2021, M.I.C.M. (C 597/19, EU:C:2021:492, **points 47 à 54).**

38 Voir, en ce sens, arrêt du 29 janvier 2008, Promusicae (C 275/06, EU:C:2008:54, points 50 à 52).

39 Voir point 65 des présentes conclusions.

40 Voir mes conclusions dans l'affaire M.I.C.M. (C 597/19, EU:C:2020:1063, point 103).

41 Voir article 15, paragraphe 1, de la directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique ») (JO 2000, L 178, p. 1).

42 Voir points 60 et 61 des présentes conclusions.

43 Voir arrêt La Quadrature du Net e.a. (point 155) (italique ajouté par mes soins).

44 Voir arrêt La Quadrature du Net e.a. (point 156) (italique ajouté par mes soins).

45 Voir arrêts du 2 octobre 2018, Ministerio Fiscal (C 207/16, EU:C:2018:788, point 55), et Prokuratuur (point 32).

46 Point 47 des présentes conclusions.

47 Voir arrêts SpaceNet, (point 131) ; La Quadrature du Net e.a. (point 166), et Commissioner of An Garda Síochána e.a. (point 98).

48 Voir arrêts Tele2 (point 115) ; du 2 octobre 2018, Ministerio Fiscal (C 207/16, EU:C:2018:788, point 56), et Prokuratuur (point 33).

49 Voir points 65 et suiv. des présentes conclusions.

50 Voir arrêts Tele2 (point 118) ; Prokuratuur (point 49), et Commissioner of An Garda Síochána e.a. (point 104).

51 Voir arrêts Tele2 (point 119) ; Prokuratuur (point 50), et du Commissioner of An Garda Síochána e.a. (point 105).

52 Voir arrêts Tele2 (point 120) ; Prokuratuur (point 51), et Commissioner of An Garda Síochána e.a. (point 106).

53 Voir arrêts Tele2 et Commissioner of An Garda Síochána e.a.

54 Voir arrêt Prokuratuur.

55 Voir arrêt Prokuratuur (point 45).

56 À titre accessoire, je relève que des arguments de faisabilité plaident également contre l'obligation d'un contrôle préalable systématique. L'existence d'un système organisé de lutte contre les infractions au droit d'auteur commises en ligne, tel que celui en cause au principal, suppose la nécessité de traiter des quantités importantes de données personnelles, en adéquation avec le nombre d'infractions poursuivies, à savoir, à titre d'exemple pour l'année 2019, selon les observations du gouvernement français, 33 465 demandes d'identification d'adresse IP effectuées par la Hadopi par jour. Dans ce contexte, l'obligation d'un contrôle préalable à l'accès à ces données risquerait de compromettre, en pratique, le fonctionnement des mécanismes de lutte organisée contre la contrefaçon en ligne, remettant en question l'équilibre entre les droits des utilisateurs et ceux des auteurs.

57 Directive du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO 2016, L 119, p. 89).

58 L'ensemble de ces garanties sont prévues par les dispositions du chapitre III, titre III, de la loi n° 78 17 relative à l'informatique, aux fichiers et aux libertés, du 6 janvier 1978 (JORF du 7 janvier 1978).

59 Voir arrêts du 26 octobre 2017, Balgarska energiyna borsa (C 347/16, EU:C:2017:816, point 31) ; du 31 mai 2018, Confetra e.a. (C 259/16 et C 260/16, EU:C:2018:370, point 63), et du 17 octobre 2019, Elektrorazpredelenie Yug (C 31/18, EU:C:2019:868, point 32).