Recueil de la jurisprudence

CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. MACIEJ SZPUNAR
présentées le 28 septembre 2023[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. À la demande de la grande chambre, présentée en application de l'article 60, paragraphe 3, du règlement de procédure de la Cour, cette dernière a décidé, le 7 mars 2023, de renvoyer la présente affaire à l'assemblée plénière.

2. Par ordonnance du 23 mars 2023, la Cour (assemblée plénière) a décidé la réouverture de la phase orale de la procédure et a invité les intéressés visés à l'article 23 du statut de la Cour de justice de l'Union européenne, le Contrôleur européen à la protection des données (CEPD) et l'Agence de l'Union européenne pour la cybersécurité (ENISA) à participer à une nouvelle audience.

3. J'avais, le 27 octobre 2022, présenté mes premières conclusions dans cette affaire avant la clôture de la phase orale de la procédure. Ces nouvelles conclusions sont donc pour moi l'occasion d'approfondir certains éléments de mon raisonnement dans cette affaire aux enjeux essentiels s'agissant de la conservation et de l'accès à des données à caractère personnel.

[1] Langue originale : le français.

II. Le cadre juridique

A. Le droit de l'Union

4. 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.

[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), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la « directive 2002/58 »).

[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).

[...]

(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. [...] »

5. 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 ;

[...] »

6. 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. »

7. 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. »

8. 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.

[...] »

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

« Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive [95/46]. 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

10. 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. »

11. 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 [...] »

12. 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. »

13. 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. »

14. 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. »

15. 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. »

16. 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. »

17. 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 [...] »

18. 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 nº 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] (ci-après le "décret du 5 mars 2010")] [...] 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.

[...] »

19. 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. »

20. 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.

4 JORF du 7 mars 2010, texte nº 19.

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

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

« 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 Ier, section 3, sous-section 3) et le livre III de la partie réglementaire du même code (titre III, chapitre Ier, 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 ;

[...] »

22. 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. »

23. L'annexe du 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 communications électroniques

24. L'article L. 34-1 du code des postes et des communications électroniques, tel que modifié par l'article 17 de la loi nº 2021-998 du 30 juillet 2021 [5], dispose, à son paragraphe II bis :

« [L]es 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 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. La procédure devant la Cour

25. En réponse à l'invitation adressée aux intéressés visés à l'article 23 du statut de la Cour de justice de l'Union européenne, les requérants au principal, les gouvernements français, danois, estonien, irlandais, néerlandais, finlandais, suédois, ainsi que la Commission européenne ont répondu aux questions écrites posées par la Cour.

26. Ces mêmes parties, à l'exception du gouvernement finlandais, les gouvernements tchèque, espagnol, chypriote, letton et norvégien, ainsi que le CEPD et l'ENISA, ont participé à l'audience qui s'est tenue le 15 mai 2023.

IV. Analyse

27. Mon analyse des questions préjudicielles dans mes premières conclusions m'avait conduit à proposer à la Cour de juger que l'article 15, paragraphe 1, de la directive 2002/58 doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale permettant la

[5] JORF du 31 juillet 2021, texte nº 1. Cette version de l'article L. 34-1 de ce code, 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, nº 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 nº 2021-976-977 QPC, du 25 février 2022 (M. Habib A. et autre), le Conseil constitutionnel (France) a déclaré contraire à la Constitution française cette précédente version de l'article L. 34-1 dudit code 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).

conservation par les fournisseurs de services de communications électroniques et l'accès par une autorité administrative telle que la Hadopi [6] limités 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 d'atteintes au droit d'auteur et aux droits voisins 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.

28. Dans les présentes conclusions, je m'attacherai à approfondir certains éléments de ma précédente analyse et les points débattus lors de l'audience qui s'est tenue le 15 mai 2023, afin d'exposer les raisons pour lesquelles je maintiens tant ma proposition de réponse aux questions préjudicielles que le raisonnement y ayant conduit [7].

29. Plus particulièrement, je démontrerai que le fait de permettre la conservation et l'accès à des données d'identité civile correspondant à des adresses IP, sans contrôle préalable, afin d'identifier les auteurs d'infraction lorsque ces données constituent le seul moyen d'identification de ces derniers satisfait les exigences dégagées par la Cour s'agissant de l'examen des mesures prises au titre de l'article 15, paragraphe 1, de la directive 2002/58 (section B).

30. Ce faisant, je mettrai en évidence qu'une telle solution constitue non pas un revirement de la jurisprudence exigeante et protectrice des droits fondamentaux développée par la Cour depuis les arrêts Tele2 Sverige et Watson e.a. [8] et La Quadrature du Net e.a. [9], mais un développement nécessaire de celle-ci qui s'inscrit, selon moi, dans le prolongement des principes édictés par la Cour. Cette distinction n'est pas seulement sémantique. En effet, la solution que je propose vise non pas à remettre en cause la jurisprudence existante, mais à permettre, au nom d'un certain pragmatisme, son adaptation en des circonstances particulières et très étroitement circonscrites (section C).

31. Dans un souci de clarté et dans la mesure où les débats lors de l'audience ont démontré un besoin de précisions à cet égard, je débuterai mon analyse par un rappel du fonctionnement du mécanisme de réponse graduée opéré par la Hadopi (section A).

A. Le mécanisme de réponse graduée opéré par la Hadopi

32. La Hadopi est une autorité administrative indépendante chargée de la protection du droit d'auteur et des droits voisins contre des atteintes à ces droits commises sur Internet. Pour ce faire a été institué le mécanisme dit de « réponse graduée », dont la mise en œuvre est confiée à la commission de protection des droits de la Hadopi.

6 Le 1er janvier 2022, le Conseil supérieur de l'audiovisuel (CSA) et la Hadopi sont devenus l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom). Compte tenu de la période durant laquelle se sont déroulés les faits du litige au principal, je me référerai toutefois, dans les présentes conclusions, à la Hadopi.

7 À cet égard, je maintiens également ma proposition de reformulation des questions préjudicielles, ainsi que ma compréhension de leur objet. En effet, s'il est seulement mentionné, dans le libellé des questions préjudicielles, l'accès aux données d'identité civile correspondant à des adresses IP, la question de l'accès à ces données est toutefois indissociable de celle de leur conservation par les fournisseurs de services de communications électroniques, de sorte que l'analyse de la compatibilité avec le droit de l'Union de la conservation est un préalable nécessaire à celle de la compatibilité de l'accès. Sur ce point, voir points 45 et suiv. de mes premières conclusions. De la même façon, bien que les questions préjudicielles visent « les données d'identité civile correspondant à une adresse IP », il convient de les comprendre comme visant également l'accès aux adresses IP permettant d'identifier la source d'une connexion. Sur ce point, voir points 41 et suiv. de mes premières conclusions.

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

9 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).

33. Cette commission est saisie par des organismes d'ayants droit, au sein desquels certains agents assermentés et agréés par le ministre de la Culture collectent, sur les réseaux de pair à pair (*peer to peer*), les adresses IP des internautes qui mettent à disposition du public des œuvres sans autorisation de leurs titulaires. Des procès-verbaux sont alors dressés. Ils contiennent, notamment, l'adresse IP de l'accès à Internet utilisé pour commettre ces violations au droit d'auteur, la date et l'heure de la violation constatée, ainsi que le titre de l'œuvre en question, et sont transmis à la commission de protection des droits de la Hadopi. Il convient de souligner, à cet égard et ainsi que l'a relevé le CEPD, que le traitement des données à caractère personnel par les agents au sein des organismes d'ayants droit fait l'objet d'une autorisation de la part de la Commission nationale de l'informatique et des libertés (CNIL), l'autorité de contrôle française en matière de protection des données [10].

34. À réception des procès-verbaux, et après un contrôle automatisé visant à garantir qu'ils contiennent l'ensemble des données requises, la commission de protection des droits de la Hadopi peut obtenir des fournisseurs de service de communications électroniques l'identité, l'adresse postale, l'adresse électronique et les coordonnées téléphoniques du titulaire de l'abonnement ayant été utilisé pour commettre une infraction au droit d'auteur.

35. La Hadopi peut alors adresser à cette personne une « recommandation » informant cette personne que son accès à Internet a fait l'objet d'une utilisation contraire au droit d'auteur et consistant à enjoindre à la personne soupçonnée d'avoir manqué à son obligation de vigilance quant au respect sur Internet des œuvres protégées par le droit d'auteur ou un droit voisin de se conformer à celle-ci. Autrement dit, la recommandation est adressée au titulaire de l'accès à Internet, qui peut être, dans les faits, une personne différente de celle ayant procédé à la mise à disposition de l'œuvre en violation du droit d'auteur. Une seconde recommandation peut être émise dans le cas d'un second constat de contrefaçon au moyen du même accès à Internet. En cas de nouvelles réitérations, la commission de protection des droits de la Hadopi peut décider de saisir le procureur de la République aux fins de poursuites pénales. À cet égard, ainsi que l'a précisé le gouvernement français dans ses premières observations, les agents de la Hadopi chargés du mécanisme de réponse graduée sont des agents assermentés et habilités par le président de la Hadopi, astreints au secret professionnel et seuls, au sein de la Hadopi, autorisés à accéder aux données personnelles traitées dans le cadre de ce mécanisme.

36. Il me faut préciser, à cet égard, que sont récoltées et transmises à la Hadopi non pas les données de l'ensemble des utilisateurs des réseaux de pair à pair lorsque ces derniers se limitent à télécharger de tels contenus [11], mais uniquement celles de personnes ayant procédé à la mise à disposition de contenus contrefaisants, c'est-à-dire ayant *téléversé* de tels contenus.

37. À titre d'illustration, pour l'année 2021, la Hadopi a ainsi reçu de la part des organismes d'ayants droit près de quatre millions de procès-verbaux, a procédé à l'envoi de 210 595 premières recommandations et de 53 564 secondes recommandations et a saisi le procureur de la République dans 1 484 cas.

[10] Voir, à cet égard, délibération n° 2010-225 de la CNIL, du 10 juin 2010, modifiant l'autorisation de mise en œuvre par la Société des auteurs, compositeurs et éditeurs de musique (SACEM) d'un traitement de données à caractère personnel ayant pour finalité la recherche et la constatation des délits de contrefaçon commis via les réseaux d'échanges de fichiers dénommés « peer to peer » (autorisation n° 1425421).

[11] Concernant le fonctionnement des réseaux de pair à pair et les différents profils d'internautes sur ces réseaux, voir mes conclusions dans l'affaire M.I.C.M. (C-597/19, EU:C:2020:1063, points 37 et suiv.).

38. Ces rappels effectués, je démontrerai en quoi un tel mécanisme, qui suppose la conservation et l'accès à des données d'identité civile correspondant à des adresses IP, satisfait, selon moi, les exigences de la jurisprudence relative aux mesures nationales prises au titre de l'article 15, paragraphe 1, de la directive 2002/58.

B. Le respect des exigences issues de la jurisprudence de la Cour relative à l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58

39. Ayant déjà, dans mes premières conclusions, procédé à un rappel de la jurisprudence de la Cour relative à la conservation et à l'accès des adresses IP attribuées à la source d'une connexion [12], je me concentrerai, dans les présentes conclusions, sur ce qui constitue, à mon sens, le cœur de cette jurisprudence, à savoir, d'une part, l'exigence de proportionnalité et, d'autre part, pour ce qui concerne l'accès à ces données, l'éventuelle nécessité d'un contrôle préalable par une juridiction ou une autorité administrative indépendante.

1. Sur la proportionnalité de la mesure en cause

40. Afin de déterminer la compatibilité avec le droit de l'Union d'une mesure de conservation ou d'accès à des données d'identité civile correspondant à une adresse IP, il convient, comme la Cour le souligne itérativement, de procéder à une conciliation des différents intérêts légitimes et droits en cause, que sont, d'une part, les droits à la protection de la vie privée ainsi qu'à la protection des données personnelles [13] garantis par les articles 7 et 8 de la Charte, et, d'autre part, la protection des droits et libertés d'autrui et des droits consacrés aux articles 3, 4, 6 et 7 de la Charte [14]. J'ajouterai que, dans l'affaire qui nous occupe, les droits à la protection de la vie privée et à la protection des données personnelles doivent également être conciliés avec le droit de propriété consacré à l'article 17 de la Charte, en ce que le mécanisme de réponse graduée vise in fine la protection du droit d'auteur et des droits voisins.

41. La Cour précise, à cet égard, que cette conciliation qui s'opère au titre de l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'adopter une mesure dérogeant au principe de confidentialité lorsqu'une telle mesure est « *nécessaire, appropriée et proportionnée,* au sein d'une société démocratique » (mise en italique par mes soins). Le considérant 11 de cette directive précise qu'une mesure de cette nature doit être « rigoureusement » *proportionnée* au but poursuivi [15].

42. La Cour se réfère par ailleurs au principe de proportionnalité tout au long de son raisonnement relatif à l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 et fait donc de celui-ci la clé de voûte de l'examen d'une mesure nationale de conservation ou d'accès à des données personnelles prise au titre de cette disposition.

[12] Points 53 et suiv. de mes premières conclusions.

[13] Les droits à la protection de la vie privée et à la protection des données personnelles se traduisent, dans le contexte de la directive 2002/58, par les principes de confidentialité des communications et de l'interdiction du stockage des données y afférentes qu'elle édicte.

[14] Arrêts La Quadrature du Net e.a. (points 120 à 122 ainsi que 127et 128) ; 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, points 48 et 50), ainsi que du 20 septembre 2022, SpaceNet et Telekom Deutschland (C-793/19 et C-794/19, ci-après l'« arrêt SpaceNet et Telekom Deutschland », EU:C:2022:702, points 63 et 65).

[15] Arrêts La Quadrature du Net e.a. (point 129), Commissioner of An Garda Síochána e.a. (point 51) et SpaceNet et Telekom Deutschland (point 66).

43. Une lecture plus approfondie de ce raisonnement révèle que le principe de proportionnalité comporte, dans le contexte de l'article 15, paragraphe 1, de la directive 2002/58, différents volets tenant, d'une part, à la gravité de l'ingérence dans les droits fondamentaux qu'implique la conservation ou l'accès aux données relatives au trafic et, d'autre part, à la nécessité de la mesure en cause.

44. S'agissant de la conservation et de l'accès aux identités civiles correspondant à des adresses IP par la Hadopi, je suis d'avis que tant la gravité de l'ingérence que le caractère indispensable de ces données devraient amener la Cour à moduler son examen de la proportionnalité d'une mesure nationale prise au titre de l'article 15, paragraphe 1, de la directive 2002/58.

a) La gravité relative de l'ingérence dans les droits fondamentaux

45. Il découle clairement de la jurisprudence constante de la Cour que, conformément au principe de proportionnalité, l'importance de l'objectif poursuivi par une mesure prise en vertu de l'article 15, paragraphe 1, de la directive 2002/58 doit être en relation avec la gravité de l'ingérence qui en résulte [16].

46. Plus particulièrement, la Cour a jugé, ainsi que je l'ai souligné dans mes premières conclusions, 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 » [17].

47. S'agissant des adresses IP, la Cour relève que si elles présentent un degré de sensibilité moindre que les autres données relatives au trafic, leur conservation et leur analyse constituent tout de même des ingérences graves dans les droits fondamentaux dès lors qu'elles peuvent être utilisées pour effectuer un traçage exhaustif du parcours de navigation d'un internaute et, partant, pour établir le profil détaillé de ce dernier et tirer des conclusions précises sur sa vie privée [18].

48. Dans l'affaire au principal, la conservation et l'accès à des données d'identité civile correspondant à des adresses IP visent la lutte contre les violations du droit d'auteur et des droits voisins. Or, il est clair, à mon sens, que cette lutte ne saurait relever de la lutte contre la criminalité grave [19], quand bien même le volume de ces violations aurait un caractère massif. Il existerait donc un décalage entre la gravité de l'ingérence dans les droits fondamentaux qu'implique la mesure en cause et l'objectif qu'elle poursuit.

16 Arrêts Commissioner of An Garda Síochána e.a. (point 56) et SpaceNet et Telekom Deutschland (point 71).

17 Arrêts Tele2 (point 115) ; du 2 octobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, point 56), et du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, ci-après l'« arrêt Prokuratuur », EU:C:2021:152, point 33). Voir également point 92 de mes premières conclusions.

18 Voir arrêts La Quadrature du Net e.a. (points 152 et 153), Commissioner of An Garda Síochána e.a. (point 73) et SpaceNet et Telekom Deutschland (point 103). Voir également points 63, 64 et 93 de mes premières conclusions.

19 J'ai soutenu, dans mes premières conclusions, que la notion de « criminalité grave » devrait recevoir une interprétation autonome afin d'empêcher tout contournement par les États membres des exigences établies à l'article 15, paragraphe 1, de la directive 2002/58. Je maintiens cette position. Il me faut toutefois souligner que, même si la Cour venait à juger que la définition de la notion de « criminalité grave » est laissée aux États membres, celle-ci devrait en tout état de cause être établie dans les limites du droit de l'Union et ne pourrait être étendue au point de vider cette disposition de sa substance.

49. Dans mes premières conclusions, j'ai, conformément à la jurisprudence de la Cour, estimé 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. Si j'ai également considéré que la conservation et l'accès à ces données devaient néanmoins être permis en l'espèce, il me faut, à la suite de l'audience, apporter encore quelques précisions.

50. Le mécanisme de réponse graduée permet à la Hadopi de mettre en relation l'adresse IP communiquée par les organisations d'ayants droit de personnes suspectées d'avoir utilisé leur accès à Internet pour commettre une violation du droit d'auteur sur un réseau de pair à pair avec l'identité civile de cette personne, ainsi qu'un extrait du fichier téléversé en violation du droit d'auteur. Ainsi que l'ont relevé la Commission et le CEPD lors de l'audience, de tels éléments, s'ils permettent d'obtenir assurément plus d'informations que la seule identité de l'auteur présumé d'une infraction, ne conduisent toutefois pas à tirer des conclusions très précises sur la vie privée de cette personne. En effet, comme je l'avais évoqué dans mes premières conclusions [20], il s'agit seulement de la révélation d'une consultation ponctuelle d'un contenu qui, pris isolément, ne saurait permettre d'établir le profil détaillé de la personne y ayant procédé.

51. Il en va d'autant plus ainsi que, tout d'abord, la grande majorité des adresses IP communiquées à la Hadopi sont des adresses IP dites « dynamiques », qui sont, par nature, changeantes et ne correspondent à une identité précise qu'à un seul moment, qui coïncide avec la mise à disposition du contenu en cause. Elles excluent donc tout traçage exhaustif.

52. Ensuite, il me faut souligner que la protection des droits fondamentaux sur Internet ne me semble pas pouvoir justifier qu'on ne puisse accéder aux seules données relatives à l'adresse IP, au contenu d'une œuvre, et à l'identité de la personne ayant procédé à sa mise à disposition en violation du droit d'auteur, mais seulement que des garanties doivent entourer la conservation et l'accès à ces dernières. Une analogie avec le monde réel me semble à cet égard éloquente : une personne soupçonnée d'avoir commis un vol ne saurait invoquer son droit à la protection de la vie privée afin que les personnes chargées de la poursuite de cette infraction ne puissent prendre connaissance du contenu volé. En revanche, cette personne peut, à raison, invoquer ses droits fondamentaux afin d'empêcher, au cours de la procédure, l'accès à un ensemble de données plus larges que les seules données nécessaires à la qualification de la prétendue infraction.

53. Enfin, je relève que, contrairement à ce qu'ont fait valoir les requérants, le mécanisme de réponse graduée ne semble pas impliquer une surveillance généralisée des utilisateurs des réseaux de pair à pair. En effet, il ne s'agit pas de vérifier l'ensemble de leur activité sur un réseau donné afin de déterminer s'ils ont procédé à une mise à disposition d'une œuvre en violation du droit d'auteur, mais plutôt, à partir d'un fichier identifié comme une contrefaçon, de déterminer le détenteur de l'accès à Internet à partir duquel l'internaute a procédé à la mise à disposition. De même, ainsi que l'a souligné le CEPD lors de l'audience, il ne s'agit pas de surveiller l'activité de l'ensemble des utilisateurs des réseaux de pair à pair, mais uniquement celle des personnes procédant au téléversement de fichiers contrefaisants, le téléversement de ces fichiers étant d'autant moins révélateur d'éléments relatifs à la vie privée de la personne qu'il peut s'effectuer uniquement pour permettre à ces internautes de procéder ensuite au téléchargement d'autres fichiers.

[20] Point 101 de mes premières conclusions.

54. Dans ces conditions, les raisons ayant conduit la Cour à considérer la conservation et l'accès aux adresses IP comme une ingérence grave dans les droits fondamentaux ne me semblent pas trouver application s'agissant d'un mécanisme de réponse graduée tel que celui opéré par la Hadopi. Il s'ensuit que la gravité de l'ingérence que cette conservation et cet accès supposent devrait, dans l'examen du principe de proportionnalité, être nuancée.

55. En d'autres termes, je suis d'avis qu'il convient d'interpréter la jurisprudence de la Cour relative à la gravité de l'ingérence dans les droits fondamentaux causée par la conservation et l'accès à des adresses IP comme impliquant non pas que cette ingérence est toujours une ingérence grave, mais qu'elle l'est seulement lorsque les adresses IP peuvent conduire à un traçage exhaustif du parcours de navigation de l'internaute et à tirer des conclusions très précises sur sa vie privée.

56. Tel n'étant pas le cas dans une situation telle que celle en cause au principal, il en résulte que l'ingérence qu'impliquent la conservation et l'accès aux identités civiles correspondant à une adresse IP utilisée pour la mise à disposition d'un contenu en violation du droit d'auteur devrait pouvoir être justifiée par un objectif de lutte contre la criminalité plus large que la seule criminalité grave.

57. Je précise en outre que l'ingérence dans les droits fondamentaux que supposent la conservation et l'accès à des données d'identité civile correspondant à une adresse IP dans une situation telle que celle en cause au principal n'est pas aggravée par la circonstance que le titulaire de l'accès à Internet utilisé pour la mise à disposition d'un contenu contrefaisant n'est pas nécessairement à l'origine de cette mise à disposition, de sorte que la recommandation adressée par la Hadopi pourrait conduire à révéler à ce titulaire ledit contenu auquel un tiers a pu accéder. D'une part, je rappelle que l'infraction recherchée par la Hadopi est celle d'un manquement à l'obligation de veiller à ce que l'accès ne fasse pas l'objet d'une utilisation à des fins de mise à disposition d'un contenu en violation du droit d'auteur. Il est donc nécessaire que les informations permettant sa qualification soient transmises à son auteur présumé. D'autre part, ainsi que je l'ai déjà énoncé, je suis d'avis que les informations relatives à l'œuvre en cause ne permettent pas de tirer de conclusions précises sur la vie privée de la personne à l'origine de la mise à disposition. La transmission éventuelle de ces informations au titulaire de la connexion Internet ne va donc pas au-delà de ce qui est nécessaire pour permettre la poursuite de l'infraction au droit d'auteur en question.

b) Le caractère indispensable des données en cause pour la détection et la poursuite d'une infraction

58. Afin d'assurer la proportionnalité d'une mesure de conservation et d'accès à des données de trafic telles que des données d'identité civile correspondant à une adresse IP prise au titre de l'article 15, paragraphe 1, de la directive 2002/58, il convient, selon la jurisprudence de la Cour, que l'ingérence qu'elle suppose soit limitée au strict nécessaire pour permettre la réalisation de l'objectif poursuivi [21]. Tel me semble être précisément le cas s'agissant de la mesure en cause au principal.

[21] Arrêts La Quadrature du Net e.a. (points 120 à 122 et 132), Commissioner of An Garda Síochána e.a. (points 48 et 54), ainsi que SpaceNet et Telekom Deutschland (points 63 et 69).

59. Ainsi que je l'ai souligné dans mes premières conclusions [22], il ressort de la jurisprudence même de la Cour que, dans le cas d'une infraction commise exclusivement en ligne, telle qu'une violation du droit d'auteur sur un réseau de pair à pair, 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 l'infraction [23]. Il en résulte, à mon sens, que la conservation et l'accès aux données d'identité civile correspondant à des adresses IP dans le but de détecter et de poursuivre les infractions au droit d'auteur commises en ligne sont, conformément à la jurisprudence, strictement nécessaires à la réalisation de l'objectif poursuivi.

60. Il est vrai que toute exigence de protection des données personnelles suppose une limitation des pouvoirs d'enquête. Cela résulte du principe même de la conciliation d'intérêts contraires, et un tel résultat ne saurait, en tant que tel, être contesté. Toutefois, dans l'hypothèse où l'adresse IP constitue le seul moyen d'identification de la personne suspectée d'avoir commis une infraction en ligne à un droit de propriété intellectuelle, une telle situation se distingue de la majorité des poursuites pénales, au sujet desquelles la Cour relève que « l'efficacité [...] dépend généralement non pas d'un seul instrument d'enquête, mais de tous les instruments d'enquête dont disposent les autorités nationales compétentes à ces fins » [24]. Admettre que les données d'identité civile correspondant à des adresses IP ne devraient pas faire l'objet d'une conservation et d'un accès dans une situation telle que celle en cause au principal ne conduirait pas, comme toute mesure assurant la protection des données de trafic, à une simple limitation des pouvoirs d'enquête, mais bien à priver les autorités nationales du seul moyen de détection et de poursuite de certaines infractions.

61. Autrement dit, il ne s'agit pas, selon l'interprétation que je propose de l'article 15, paragraphe 1, de la directive 2002/58, de permettre, par le jeu de l'examen de la nécessité d'une telle mesure, la conservation et l'accès à des données qui *facilitent* seulement la détection et la poursuite d'infractions, lorsque ces infractions peuvent également être détectées et poursuivies par des moyens concurrents, même moins efficaces. Il est en revanche question de permettre la conservation et l'accès à ces données lorsque celles-ci sont *indispensables* à l'identification de la personne suspectée d'avoir commis une infraction, qui ne pourrait être poursuivie sans ces moyens dès lors que les données en cause constituent l'unique instrument d'identification de l'internaute dans la mesure où l'infraction est exclusivement constituée en ligne.

62. Une telle interprétation s'impose, à mon sens, sauf à admettre que toute une série d'infractions pénales ne puisse jamais faire l'objet de poursuites [25].

63. Il résulte de tout ce qui précède qu'à mon sens, une réglementation nationale permettant la conservation par les fournisseurs de services de communications électroniques et l'accès par une autorité administrative limités à des données d'identité civile correspondant à des adresses IP est pleinement proportionnée à l'objectif poursuivi, à savoir la poursuite d'atteintes au droit d'auteur et aux droits voisins sur Internet, dans la mesure où l'ingérence dans les droits fondamentaux qu'ils supposent est d'une gravité limitée et où 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.

[22] Point 78 de mes premières conclusions.

[23] Arrêts La Quadrature du Net e.a. (point 154), Commissioner of An Garda Síochána e.a. (point 73), et SpaceNet et Telekom Deutschland (point 100).

[24] Arrêt Commissioner of An Garda Síochána e.a. (point 69).

[25] Point 81 de mes premières conclusions. Voir également, sur ce point, points 79 et suiv. des présentes conclusions.

64. Partant, je suis d'avis que l'article 15, paragraphe 1, de la directive 2002/58 devrait être interprété comme ne s'opposant pas à une telle réglementation.

2. Sur l'existence de garanties matérielles et procédurales adéquates

65. S'agissant spécifiquement de l'accès à des données d'identité civile correspondant à des adresses IP, il ressort de la jurisprudence de la Cour que la seule proportionnalité stricte de la mesure ne suffit pas à la rendre compatible avec l'article 15, paragraphe 1, de la directive 2002/58.

66. En effet, afin d'assurer que l'accès à des données relatives au trafic et à la localisation soit limité au strict nécessaire, la Cour a jugé qu'il est essentiel que cet accès soit subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante disposant de toutes les attributions et présentant toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts légitimes et droits en cause [26].

67. Une lecture stricte de la jurisprudence conduirait dès lors à considérer que l'accès par la Hadopi aux données d'identité civile correspondant aux adresses IP des personnes suspectées d'avoir commis une infraction au droit d'auteur sur Internet devrait être subordonné à un tel contrôle préalable, qui fait défaut dans le mécanisme de réponse graduée tel qu'il existe.

68. Cependant, ainsi que l'a fait valoir le gouvernement irlandais lors de l'audience et comme je l'ai soutenu dans mes premières conclusions, je suis d'avis que l'exigence d'un contrôle préalable par une juridiction ou par une entité administrative indépendante n'est pas une exigence systématique, mais dépend d'une analyse plus globale de la mesure en cause prenant en compte tant la gravité de l'ingérence qu'elle suppose que les garanties qu'elle prévoit.

69. En effet, je souligne que, dans chacun des arrêts ayant énoncé cette exigence d'un contrôle préalable par une juridiction ou par une entité administrative indépendante, étaient en cause des réglementations nationales permettant l'accès à l'ensemble des données de trafic et de localisation des utilisateurs relatives à tous les moyens de communication électronique d'utilisateurs [27] ou, à tout le moins, à la téléphonie fixe et mobile [28] d'utilisateurs identifiés.

70. J'en déduis que l'exigence d'un tel contrôle préalable est guidée par la gravité de l'ingérence en cause dans les affaires en question. Ainsi que la Cour l'a souligné, il s'agissait de données « effectivement susceptible[s] de permettre de tirer des conclusions précises, voire très précises, concernant la vie privée des personnes [...] 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 » [29]. De plus, étaient visées les données de personnes déjà identifiées et suspectées d'avoir commis une infraction sur la base d'autres indices, les données en cause permettant donc de renforcer les éléments à charge contre l'utilisateur en question en étendant le champ des données le concernant.

[26] Arrêts Tele2 (point 120), Prokuratuur (points 51 et 52) ainsi que Commissioner of An Garda Síochána e.a. (points 106 et 107).

[27] Arrêts Tele2 et Commissioner of An Garda Síochána e.a..

[28] Arrêt Prokuratuur.

[29] Arrêt Prokuratuur (point 36).

71. Or, s'agissant de la réglementation en cause au principal, et ainsi que je l'ai souligné, la gravité de l'ingérence que suppose la mise en relation d'une donnée d'identité civile et d'une adresse IP est bien moindre que celle résultant de l'accès à l'ensemble des données de trafic et de localisation d'une personne, dans la mesure où cette mise en relation n'apporte aucun élément permettant de tirer des conclusions précises sur la vie privée de la personne visée.

72. En outre, ainsi que je l'ai relevé dans mes premières conclusions [30], ces données ne concernent que les personnes qui, à la suite d'un constat objectif d'utilisation de l'adresse IP en violation d'un droit d'auteur établi par les organismes d'ayants droit, se sont livrées à des faits susceptibles de constituer un manquement à l'obligation de vigilance, prévue à l'article L.336-3 du CPI. Elles ne sont pas préalablement identifiées par d'autres moyens, la mise en relation de l'adresse IP avec les données d'identité civile étant le seul moyen d'identification de la personne concernée. L'accès à ces données permet donc non pas, ainsi que cela était le cas dans les affaires dont la Cour a précédemment eu à juger, d'obtenir des informations supplémentaires et précises sur l'activité de personnes déjà suspectées sur la base d'autres éléments, mais seulement de rendre exploitable l'adresse IP, autrement dépourvue d'intérêt. Dans ces conditions, les données auxquelles la Hadopi a accès sont de facto limitées.

73. Il existe, selon moi, une différence fondamentale entre le fait d'accéder à des données à caractère personnel relatives à une personne suspectée d'avoir commis une infraction afin de démontrer sa culpabilité et celui de permettre de dévoiler l'identité de l'auteur d'une infraction déjà constatée.

74. Il en va d'autant plus ainsi, à mon sens, que le recueil des adresses IP sur les réseaux de pair à pair fait l'objet d'une autorisation préalable limitée à ces seules données, de sorte que la Hadopi n'est jamais en possession d'un ensemble illimité de données s'agissant des internautes suspectés d'avoir commis une infraction au droit d'auteur sur Internet [31].

75. Partant, la logique qui sous-tend l'exigence d'un contrôle préalable opéré par une juridiction ou une entité administrative indépendante ne trouve pas application s'agissant du mécanisme de réponse graduée tel que celui en cause au principal, de sorte qu'une telle exigence ne m'apparaît pas nécessaire pour assurer que l'ingérence dans les droits fondamentaux qu'implique ce mécanisme est limitée au strict nécessaire.

76. Il résulte de tout ce qui précède qu'une réglementation nationale permettant la conservation et l'accès par une autorité administrative indépendante telle que la Hadopi à des données d'identité civile correspondant à des adresses IP afin d'identifier les titulaires de ces adresses soupçonnés d'être responsables d'atteintes au droit d'auteur, sans que cet accès soit subordonné à un contrôle préalable par une juridiction ou une entité administrative indépendante respecte, in fine, les principes édictés par la jurisprudence de la Cour, lorsque ces données constituent le seul moyen d'identification de la personne à laquelle l'adresse IP était attribuée au moment de la commission de l'infraction, de sorte que l'article 15, paragraphe 1, de la directive 2002/58 devrait être interprété comme ne s'opposant pas à une telle réglementation.

77. Au-delà de ces considérations propres à l'affaire en cause au principal, il me faut encore formuler des remarques plus générales sur la nécessité de procéder à ce développement de la jurisprudence de la Cour.

30 Point 102 de mes premières conclusions.

31 Point 33 des présentes conclusions.

C. Un développement de la jurisprudence nécessaire et limité

78. Plusieurs arguments militent en faveur d'un raffinement de la jurisprudence de la Cour relative à la conservation et à l'accès à des données telles que les adresses IP couplées à des données d'identité civile.

79. En premier lieu, et ainsi que je l'ai déjà souligné [32], dans la situation en cause au principal, l'obtention des données d'identité civile correspondant à une adresse IP est 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 en cause.

80. Il en résulte nécessairement que si la Cour était amenée à considérer que l'article 15, paragraphe 1, de la directive 2002/58 s'oppose tout de même à leur conservation et à leur accès, les autorités nationales seraient de facto privées de ce seul moyen d'identification et, par là même, les auteurs de l'infraction en question ne pourraient jamais être poursuivis [33]. Cela m'a conduit, dans mes premières conclusions, à évoquer la possibilité d'une impunité systémique pour cette infraction [34].

81. Le risque d'une impunité systémique n'est pas limité aux infractions au droit d'auteur commises sur les réseaux de pair à pair, mais s'étend, ainsi que l'a fait valoir le gouvernement tchèque lors de l'audience, à l'ensemble des infractions exclusivement constituées en ligne.

82. En effet, les infractions dont l'auteur peut seulement être identifié par l'intermédiaire de son adresse IP ne pourraient jamais être poursuivies et les textes qui les sanctionnent jamais appliqués s'il devait être jugé que tant la conservation des données que l'accès à celles-ci sont contraires au droit de l'Union.

83. À cet égard, je relève qu'il est vrai, ainsi que l'ont avancé les requérants au principal, que d'autres moyens pourraient permettre, en théorie, d'identifier les auteurs de certaines infractions exclusivement commises en ligne. Ainsi, elles se réfèrent notamment à l'identifiant utilisé sur les réseaux sociaux et aux données associées au compte de l'utilisateur, son adresse courriel, son numéro de téléphone, ou un élément sur sa vie privée que la personne aurait révélés. Cependant, de telles données nécessitent, afin de les lier à l'identité de la personne, des investigations approfondies, au cours desquelles est examinée l'activité en ligne de l'internaute. Le recours à de tels moyens d'investigation me semble donc susceptible de permettre de tirer, à la différence de la seule adresse IP, des conclusions très précises sur la vie privée des personnes, de sorte que la conservation et l'accès à ces données seraient, en ce sens, contraires à l'article 15, paragraphe 1, de la directive 2002/58.

84. Dans ces conditions, l'accès à des données d'identité civile correspondant à l'adresse IP d'un internaute n'est certes pas l'unique moyen théorique d'investigation permettant l'identification de la personne titulaire de cette adresse au moment de la commission de l'infraction, mais celui permettant sa poursuite tout en impliquant la moindre ingérence dans les droits fondamentaux de celle-ci et, partant, d'échapper à une impunité générale.

[32] Point 59 des présentes conclusions.

[33] Point 62 des présentes conclusions.

[34] Points 78 et suiv. de mes premières conclusions.

85. En deuxième lieu, je souligne à nouveau qu'une telle solution permettrait, à mon sens, de réconcilier deux lignes de jurisprudence de la Cour, sources d'une certaine tension que j'avais identifiée dans mes premières conclusions [35] et dans celles relatives à l'affaire M.I.C.M. [36], à savoir, d'une part, la jurisprudence relative à la conservation et à l'accès aux données et, d'autre part, celle 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, initiés par des personnes privées.

86. En troisième lieu, si la jurisprudence de la Cour depuis les arrêts Tele2 et La Quadrature du Net e.a se doit d'être saluée en ce qu'elle a permis la mise en place d'un cadre protecteur des droits fondamentaux des utilisateurs de services de communications électroniques, elle est néanmoins empreinte d'une certaine casuistique. En effet, au fil des affaires soumises à son examen, la Cour a procédé à un raffinement progressif de sa jurisprudence lui permettant d'examiner diverses réglementations nationales à la lumière de l'article 15, paragraphe 1, de la directive 2002/58. Toutefois, il est impossible pour la Cour d'anticiper virtuellement toutes les mesures qui pourraient faire l'objet d'une analyse à la lumière de cette disposition. En témoigne d'ailleurs le nombre de renvois préjudiciels [37] dont cette dernière fait l'objet depuis l'arrêt Tele2, qui atteste, à mon sens, de la difficulté que peuvent éprouver les juridictions nationales à appliquer les principes énoncés dans la jurisprudence de la Cour à des situations différentes de celles ayant donné lieu aux arrêts en question [38].

87. Il en résulte donc qu'une certaine souplesse m'apparaît nécessaire lorsque sont soumises à l'examen de la Cour des mesures qui ne pouvaient être envisagées lors de précédents arrêts – telles que des réglementations visant des infractions pouvant n'être poursuivies que dans la mesure où les données d'identité civile correspondant à des adresses IP sont conservées et accessibles –, dont la Cour n'a, jusqu'à présent, jamais eu à connaître.

88. Il ne s'agit donc pas, comme l'avait défendu le gouvernement danois, de reconsidérer la jurisprudence de la Cour, mais d'admettre que, sur la base des principes qui la sous-tendent, une solution plus nuancée puisse être dégagée, dans des circonstances très limitées.

89. En effet, l'interprétation que je propose de l'article 15, paragraphe 1, de la directive 2002/58 ne permet la conservation et l'accès à des données d'identité civile correspondant à des adresses IP que pour ce qui concerne la poursuite d'infractions dont les auteurs ne pourraient, en l'absence de ces données, pas être identifiés. Elle vise donc uniquement les infractions constituées exclusivement sur Internet et ne remet pas en cause les solutions énoncées dans la jurisprudence relatives à la conservation et à l'accès à des données plus larges, et poursuivant d'autres objectifs.

35 Points 69 et suiv. de mes premières conclusions.

36 C-597/19, EU:C:2020:1063.

37 Arrêts du 2 octobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788) ; La Quadrature du Net e.a. ; Prokuratuur ; Commissioner of An Garda Síochána e.a. ainsi que SpaceNet et Telekom Deutschland.

38 À cet égard, la multiplication des demandes de décisions préjudicielles ayant pour objet l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 peut également indiquer une certaine forme de réticence de la part des juridictions nationales à appliquer les principes dégagés par la Cour à des situations légèrement différentes, en raison des spécificités des ordres juridiques nationaux. Sur ce point, voir notamment Cameron, I., « Metadata retention and national security : *Privacy international* and *La Quadrature du Net* », *Common Market Law Review*, 2021, vol. 58, nº 5, p. 1433 à 1471, ou encore Bertrand, B., « L'audace sans le tact : jusqu'où la Cour de justice peut-elle aller trop loin ? », *Dalloz IP/IT*, 2021, nº 9, p. 468 à 472. Il me semble dès lors d'autant plus essentiel, dans la perspective de maintenir un dialogue fructueux entre la Cour et les juridictions des États membres, que la Cour puisse faire preuve d'adaptation quand les circonstances le commandent. Ainsi que l'ont relevé les auteurs de la doctrine, le standard élevé de protection institué par la jurisprudence de la Cour ne saurait être réellement efficace sans adhésion de la part des juridictions nationales, en charge, au premier chef, de le mettre en œuvre. Sur ce point, voir notamment Teyssedre, J., « Strictly regulated retention and access regimes for metadata : *Commissioner of An Garda Siochana* », *Common Market Law Review*, vol. 60, nº 2, 2023, p. 569 à 588, et Sirinelli, J., « La protection des données de connexion par la Cour de justice : cartographie d'une jurisprudence européenne inédite », *Revue trimestrielle de droit européen*, vol. 57, nº 2, 2021, p. 313 à 329.

V. Conclusion

90. 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), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne,

doit être interprété en ce sens 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 du droit d'auteur et des droits voisins contre des atteintes à ces droits commises sur Internet limités 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 des personnes auxquelles lesdites adresses étaient attribuées au moment de la commission de l'infraction.