ARRÊT DE LA COUR (assemblée plénière)

30 avril 2024 (*)

Table des matières

Le cadre juridique
- Le droit de l'Union
  - La réglementation générale relative à la protection des données à caractère personnel
    - – La directive 95/46/CE
    - – Le RGPD
  - La réglementation sectorielle relative à la protection des données à caractère personnel
    - – La directive 2002/58
    - – La directive (UE) 2016/680
  - La réglementation relative à la protection des droits de propriété intellectuelle
- Le droit français
  - Le CPI
  - Le décret n o 2010-236
  - Le code des postes et des communications électroniques

Le litige au principal et les questions préjudicielles

Sur les questions préjudicielles
- Observations liminaires
- Sur l'existence d'une justification au titre de l'article 15, paragraphe 1, de la directive 2002/58 de l'accès d'une autorité publique à des données relatives à l'identité civile correspondant à une adresse IP conservées par les fournisseurs de services de communications électroniques aux fins de la lutte contre la contrefaçon commise en ligne
  - Sur les exigences entourant la conservation des données relatives à l'identité civile et des adresses IP correspondantes par les fournisseurs de services de communications électroniques
  - Sur les exigences entourant l'accès aux données relatives à l'identité civile correspondant à une adresse IP conservées par les fournisseurs de services de communications électroniques
  - Sur l'exigence d'un contrôle par une juridiction ou une entité administrative indépendante préalablement à l'accès par une autorité publique à des données relatives à l'identité civile correspondant à une adresse IP
  - Sur les exigences tenant aux conditions matérielles et procédurales ainsi qu'aux garanties contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données s'imposant à l'accès par une autorité publique à des données relatives à l'identité civile correspondant à une adresse IP

Sur les dépens

« Renvoi préjudiciel – Traitement des données à caractère personnel et protection de la vie privée dans le secteur des communications électroniques – Directive 2002/58/CE – Confidentialité des communications électroniques – Protection – Article 5 et article 15, paragraphe 1 – Charte des droits fondamentaux de l'Union européenne – Articles 7, 8 et 11 et article 52, paragraphe 1 – Législation nationale visant à combattre, par l'action d'une autorité publique, les contrefaçons commises sur Internet – Procédure dite de "réponse graduée" – Collecte en amont par des organismes d'ayants droit des adresses IP utilisées pour des activités portant atteinte aux droits d'auteur ou aux droits voisins – Accès en aval de l'autorité publique chargée de la protection des droits d'auteur et des droits voisins à des données relatives à l'identité civile correspondant à ces adresses IP conservées par les fournisseurs de services de communications électroniques – Traitement automatisé – Exigence d'un contrôle préalable par une juridiction ou une entité administrative indépendante – Conditions matérielles et procédurales – Garanties contre les risques d'abus ainsi que contre tout accès à ces données et toute utilisation illicites de celles-ci »

Dans l'affaire C-470/21,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par le Conseil d'État (France), par décision du 5 juillet 2021, parvenue à la Cour le 30 juillet 2021, dans la procédure

La Quadrature du Net,

Fédération des fournisseurs d'accès à Internet associatifs,

Franciliens.net,

French Data Network

contre

Premier ministre,

Ministre de la Culture,

LA COUR (assemblée plénière),

composée de M. K. Lenaerts, président, M. L. Bay Larsen, vice-président, M. A. Arabadjiev, M^mes^ A. Prechal (rapporteure), K. Jürimäe, MM. C. Lycourgos, E. Regan, T. von Danwitz, F. Biltgen, N. Piçarra et Z. Csehi, présidents de chambre, MM. M. Ilešič, J.-C. Bonichot, S. Rodin, P. G. Xuereb, M^me^ L. S. Rossi, MM. I. Jarukaitis, A. Kumin, N. Jääskinen, N. Wahl, M^me^ I. Ziemele, MM. J. Passer, D. Gratsias, M^me^ M. L. Arastey Sahún et M. M. Gavalec, juges,

avocat général : M. M. Szpunar,

greffiers : M^mes^ V. Giacobbo et M. Krausenböck, administratrices,

vu la procédure écrite et à la suite de l'audience du 5 juillet 2022,

considérant les observations présentées :

– pour La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net et French Data Network, par M^e^ A. Fitzjean Ó Cobhthaigh, avocat,

– pour le gouvernement français, par M^mes^ A. Daniel, A.-L. Desjonquères et M. J. Illouz, en qualité d'agents,

– pour le gouvernement danois, par M^mes^ J. F. Kronborg et V. Pasternak Jørgensen, en qualité d'agents,

– pour le gouvernement estonien, par M^me^ M. Kriisa, en qualité d'agent,

– pour le gouvernement finlandais, par M^me^ H. Leppo, en qualité d'agent,

– pour le gouvernement suédois, par M^me^ H. Shev, en qualité d'agent,

– pour le gouvernement norvégien, par MM. F. Bergsjø, S.-E. Dahl, M^me^ J. T. Kaasin et M. P. Wennerås, en qualité d'agents,

– pour la Commission européenne, par MM. S. L. Kalėda, H. Kranenborg, P.-J. Loewenthal et F. Wilman, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 27 octobre 2022,

vu l'ordonnance de réouverture de la procédure orale du 23 mars 2023 et à la suite de l'audience du 15 mai 2023,

considérant les observations présentées :

– pour La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net et French Data Network, par M^e^ A. Fitzjean Ó Cobhthaigh, avocat,

– pour le gouvernement français, par MM. R. Bénard, J. Illouz et T. Stéhelin, en qualité d'agents,

– pour le gouvernement tchèque, par M^me^ T. Suchá et M. J. Vláčil, en qualité d'agents,

– pour le gouvernement danois, par M^mes^ J. F. Kronborg et C. A.-S. Maertens, en qualité d'agents,

– pour le gouvernement estonien, par M^me^ M. Kriisa, en qualité d'agent,

– pour l'Irlande, par M^me^ M. Browne, Chief State Solicitor, MM. A. Joyce et D. O'Reilly, en qualité d'agents, assistés de M. D. Fenelly, BL,

– pour le gouvernement espagnol, par M^me^ A. Gavela Llopis, en qualité d'agent,

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

– pour le gouvernement letton, par M^mes^ J. Davidoviča et K. Pommere, en qualité d'agents,

– pour le gouvernement néerlandais, par M^mes^ E. M. M. Besselink, M. K. Bultermann et A. Hanje, en qualité d'agents,

– pour le gouvernement finlandais, par M^mes^ A. Laine et H. Leppo, en qualité d'agents,

– pour le gouvernement suédois, par M^mes^ F.-D. Göransson et H. Shev, en qualité d'agents,

– pour le gouvernement norvégien, par MM. S.-E. Dahl et P. Wennerås, en qualité d'agents,

– pour la Commission européenne, par MM. S. L. Kalėda, H. Kranenborg, P.-J. Loewenthal et F. Wilman, en qualité d'agents,

– pour le Contrôleur européen de la protection des données, par MM. V. Bernardo, M^me^ C.-A. Marnier, MM. D. Nardi et M. Pollmann, en qualité d'agents,

– pour l'Agence de l'Union européenne pour la cybersécurité, par M^me^ A. Bourka, en qualité d'agent,

ayant entendu l'avocat général en ses conclusions à l'audience du 28 septembre 2023,

rend le présent

Arrêt

1 La demande de décision préjudicielle porte sur l'interprétation de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la « directive 2002/58 »), lue à la lumière de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

2 Cette demande a été présentée dans le cadre d'un litige opposant La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net et French Data Network, des associations, au Premier ministre (France) et au ministre de la Culture (France) au sujet de la légalité 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 code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet » (JORF nº 56 du 7 mars 2010, texte nº 19), tel que modifié par le décret nº 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (JORF nº 109 du 10 mai 2017, texte nº 176) (ci-après le « décret nº 2010-236 »).

Le cadre juridique

Le droit de l'Union

La réglementation générale relative à la protection des données à caractère personnel

– *La directive 95/46/CE*

3 Figurant dans la section II, intitulée « Principes relatifs à la légitimation des traitements de données », du chapitre II de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31), l'article 7 de celle-ci était ainsi libellé :

« Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si :

[...]

f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1. »

4 L'article 13, paragraphe 1, de ladite directive disposait :

« Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11, paragraphe 1, et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder :

[...]

g) la protection de la personne concernée ou des droits et libertés d'autrui. »

– *Le RGPD*

5 L'article 2 du règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO 2016, L 119, p. 1, ci-après le « RGPD »), intitulé « Champ d'application matériel », dispose, à ses paragraphes 1 et 2 :

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

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

[...]

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

6 L'article 4 du RGPD, intitulé « Définitions », précise :

« Aux fins du présent règlement, on entend par :

1) "données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; [...]

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

[...] »

7 L'article 6 de ce règlement, intitulé « Licéité du traitement », prévoit, à son paragraphe 1 :

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

[...]

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel [...]

Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions. »

8 L'article 9 dudit règlement, intitulé « Traitement portant sur des catégories particulières de données à caractère personnel », prévoit, à son paragraphe 2, sous e) et f), que l'interdiction du traitement de certains types de données à caractère personnel qui révèle notamment des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ne s'applique pas lorsque le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ou est nécessaire notamment à la constatation, à l'exercice ou à la défense d'un droit en justice.

9 L'article 23 du RGPD, intitulé « Limitations », dispose, à son paragraphe 1 :

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

[...]

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

j) l'exécution des demandes de droit civil. »

La réglementation sectorielle relative à la protection des données à caractère personnel

– *La directive 2002/58*

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

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

[...]

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

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

[...]

(11) À l'instar de la directive [95/46], la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit 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.

[...]

(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. [...] »

11 Aux termes de l'article 2 de la directive 2002/58, 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 ;

[...] »

12 L'article 3 de cette directive, intitulé « Services concernés », prévoit :

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

13 Aux termes de l'article 5 de ladite directive, intitulé « Confidentialité des communications » :

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

[...]

3. Les États membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive [95/46], une information claire et complète, entre autres sur les finalités du traitement. […] »

14 L'article 6 de la même directive, intitulé « Données relatives au trafic », dispose :

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

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

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

[…]

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

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

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

[…]

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

[…] »

– *La directive (UE) 2016/680*

16 L'article 1er de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO 2016, L 119, p. 89), intitulé « Objet et objectifs », prévoit, à son paragraphe 1 :

« La présente directive établit des règles relatives 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. »

17 L'article 3 de ladite directive, intitulé « Définitions », dispose :

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

[...]

7. "autorité compétente" :

a) toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ; ou

b) tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;

[...] »

La réglementation relative à la protection des droits de propriété intellectuelle

18 L'article 8 de la directive 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle (JO 2004, L 157, p. 45, et rectificatif JO 2004, L 195, p. 16), intitulé « Droit d'information », dispose :

« 1. Les États membres veillent à ce que, dans le cadre d'une action relative à une atteinte à un droit de propriété intellectuelle et en réponse à une demande justifiée et proportionnée du requérant, les autorités judiciaires compétentes puissent ordonner que des informations sur l'origine et les réseaux de distribution des marchandises ou des services qui portent atteinte à un droit de propriété intellectuelle soient fournies par le contrevenant [...]

2. Les informations visées au paragraphe 1 comprennent, selon les cas :

a) les noms et adresses des producteurs, fabricants, distributeurs, fournisseurs et autres détenteurs antérieurs des marchandises ou des services, ainsi que des grossistes destinataires et des détaillants ;

[...]

3. Les paragraphes 1 et 2 s'appliquent sans préjudice d'autres dispositions législatives et réglementaires qui :

a) accordent au titulaire le droit de recevoir une information plus étendue ;

b) régissent l'utilisation au civil ou au pénal des informations communiquées en vertu du présent article ;

c) régissent la responsabilité pour abus du droit à l'information ;

d) donnent la possibilité de refuser de fournir des informations qui contraindraient la personne visée au paragraphe 1 à admettre sa propre participation ou celle de ses proches parents à une atteinte à un droit de propriété intellectuelle ; ou

e) régissent la protection de la confidentialité des sources d'information ou le traitement des données à caractère personnel. »

Le droit français

Le CPI

19 L'article L. 331-12 du code de la propriété intellectuelle, dans sa rédaction en vigueur à la date de la décision contestée par les requérantes au principal (ci-après le « CPI »), dispose :

« La Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet [(Hadopi)] est une autorité publique indépendante. […] »

20 L'article L. 331-13 de ce code prévoit :

« La [Hadopi] assure :

1° Une mission d'encouragement au développement de l'offre légale et d'observation de l'utilisation licite et illicite des œuvres et des objets auxquels est attaché un droit d'auteur ou un droit voisin sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne ;

2° Une mission de protection de ces œuvres et objets 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 ;

[…] »

21 Aux termes de l'article L. 331-15 dudit 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. »

22 L'article L. 331-17, premier alinéa, du même code dispose :

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

23 Aux termes de l'article L. 331-21 du CPI :

« 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 nº 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. »

24 L'article L. 331-24 de ce code 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. »

25 Aux termes de l'article L. 331-25 dudit code, qui régit 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. »

26 L'article L. 331-29 du CPI 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 [...] »

27 L'article L. 335-2, premier et deuxième alinéas, de ce code précise :

« Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit.

La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende. »

28 L'article L. 335-4, premier alinéa, dudit code énonce :

« Est punie de trois ans d'emprisonnement et de 300 000 euros d'amende toute fixation, reproduction, communication ou mise à disposition du public, à titre onéreux ou gratuit, ou toute télédiffusion d'une prestation, d'un phonogramme, d'un vidéogramme, d'un programme ou d'une publication de presse, réalisée sans l'autorisation, lorsqu'elle est exigée, de l'artiste-interprète, du producteur de phonogrammes ou de vidéogrammes, de l'entreprise de communication audiovisuelle, de l'éditeur de presse ou de l'agence de presse. »

29 L'article L. 335-7 du CPI prescrit les règles relatives à l'imposition aux personnes coupables des infractions pénales visées notamment aux articles L. 335-2 et L. 335-4 de ce code de la peine complémentaire de suspension de l'accès à un service de communication au public en ligne pour une durée maximale d'un an.

30 L'article L. 335-7-1, premier alinéa, dudit code se lit comme suit :

« Pour les contraventions de la cinquième classe prévues par le présent code, lorsque le règlement le prévoit, la peine complémentaire définie à l'article L. 335-7 peut être prononcée selon les mêmes modalités, en cas de négligence caractérisée, à l'encontre du titulaire de l'accès à un service de communication au public en ligne auquel la commission de protection des droits, en application de l'article L. 331-25, a préalablement adressé, par voie d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation, une recommandation l'invitant à mettre en œuvre un moyen de sécurisation de son accès à internet. »

31 Aux termes de l'article L. 336-3 du même code :

« 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 [...] »

32 L'article R. 331-37, premier alinéa, du CPI 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] 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. »

33 Aux termes de l'article R. 331-40 de ce code :

« Lorsque, dans le délai d'un an suivant la présentation de la recommandation mentionnée au premier alinéa de l'article L. 335–7–1, la commission de protection des droits est saisie de nouveaux faits susceptibles de constituer une négligence caractérisée définie à l'article R. 335-5, elle informe l'abonné, par lettre remise contre signature, que ces faits sont susceptibles de poursuite. Cette lettre invite l'intéressé à présenter ses observations dans un délai de quinze jours. Elle précise qu'il peut, dans le même délai, solliciter une audition en application de l'article L. 331–21–1 et qu'il a droit de se faire assister par un conseil. Elle l'invite également à préciser ses charges de famille et ses ressources.

La commission peut de sa propre initiative convoquer l'intéressé aux fins d'audition. La lettre de convocation précise qu'il a droit de se faire assister par un conseil. »

34 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. »

35 À compter du 1er janvier 2022, en application de la loi nº 2021-1382, du 25 octobre 2021, relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique (JORF nº 250, du 26 octobre 2021, texte nº 2), la Hadopi a été fusionnée avec le Conseil supérieur de l'audiovisuel (CSA), autre autorité publique indépendante, pour constituer l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM).

36 La procédure de réponse graduée, mentionnée au point 25 du présent arrêt, est toutefois restée en substance inchangée même si elle est dorénavant mise en œuvre non plus par la commission de protection des droits

de la Hadopi, qui était composée de trois membres désignés respectivement par le Conseil d'État, la Cour des comptes et la Cour de cassation, mais par deux membres du collège de l'ARCOM dont l'un est désigné par le Conseil d'État et l'autre par la Cour de cassation.

Le décret nº 2010-236

37 Le décret nº 2010-236, pris notamment sur le fondement de l'article L. 331-29 du CPI, prévoit, à son article 1er :

« Le traitement de données à caractère personnel dénommé "Système de gestion des mesures pour la protection des œuvres sur 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 ;

[...] »

38 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. »

39 L'annexe audit décret 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.

[…] »

Le code des postes et des communications électroniques

40 L'article L. 34-1, II bis, du code des postes et des communications électroniques dispose :

« 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 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. »

Le litige au principal et les questions préjudicielles

41 Le Premier ministre ayant implicitement rejeté leur demande tendant à l'abrogation du décret nº 2010-236, les requérantes au principal ont, par une requête du 12 août 2019, saisi le Conseil d'État (France) d'un recours tendant à l'annulation de cette décision implicite de rejet. Elles ont fait valoir, en substance, que l'article L. 331-21, troisième à cinquième alinéas, du CPI, qui fait partie de la base légale de ce décret, d'une part, est contraire au droit au respect de la vie privée consacré par la Constitution française et, d'autre part, méconnaît le droit de l'Union, en particulier l'article 15 de la directive 2002/58 ainsi que les articles 7, 8, 11 et 52 de la Charte.

42 En ce qui concerne l'aspect du recours relatif à la violation alléguée de la Constitution, le Conseil d'État a saisi le Conseil constitutionnel (France) d'une question prioritaire de constitutionnalité.

43 Par sa décision nº 2020-841 QPC du 20 mai 2020, La Quadrature du Net et autres [Droit de communication à la Hadopi], le Conseil constitutionnel a déclaré contraires à la Constitution les troisième et quatrième alinéas de l'article L. 331-21 du CPI, mais a déclaré conforme à celle-ci le cinquième alinéa dudit article à l'exception du mot « notamment » y figurant.

44 S'agissant de l'aspect du recours relatif à la méconnaissance alléguée du droit de l'Union, les requérantes au principal ont soutenu, en particulier, que le décret nº 2010-236 et les dispositions qui en constituent la base légale autorisent l'accès à des données de connexion de façon disproportionnée pour des infractions relatives aux droits d'auteur et commises sur Internet qui sont dépourvues de gravité, sans contrôle préalable d'un juge ou d'une autorité présentant des garanties d'indépendance et d'impartialité. En particulier, ces infractions ne relèveraient pas de la « criminalité grave » visée par l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970).

45 À cet égard, le Conseil d'État rappelle, d'une part, que, par l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), la Cour a dit pour droit, notamment, 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, 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. Partant, s'agissant des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, une telle conservation serait possible, sans délai particulier, à des fins de recherche, de détection et de poursuite des infractions pénales en général. La directive 2002/58 ne s'opposerait pas davantage à un accès à ces données à de telles fins.

46 La juridiction de renvoi en déduit que, s'agissant de l'accès à des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, le moyen des requérantes au principal tiré de ce que le décret nº 2010-236 est illégal en ce qu'il a été pris dans le cadre de la lutte contre des infractions dépourvues de gravité devrait être écarté.

47 Elle rappelle, d'autre part, que, par l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), la Cour a dit pour droit, notamment, que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à 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 entité administrative indépendante.

48 La juridiction de renvoi fait référence, plus spécifiquement, au point 120 de cet arrêt, par lequel la Cour a précisé qu'il est essentiel qu'un tel accès 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.

49 La Cour aurait rappelé cette exigence dans l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), en ce qui concerne le recueil en temps réel des données de connexion par les services de renseignement, ainsi que dans l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux

données relatives aux communications électroniques) (C-746/18, EU:C:2021:152), s'agissant de l'accès des autorités nationales aux données de connexion.

50 La juridiction de renvoi fait également observer que la Hadopi, depuis sa création au cours de l'année 2009, a adressé plus de 12,7 millions de recommandations à des titulaires d'abonnement 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. Cette circonstance impliquerait que les agents de la commission de la protection des droits de la Hadopi ont nécessairement dû recueillir, chaque année, un nombre considérable de données relatives à l'identité civile des utilisateurs concernés. Elle estime que, eu égard au volume de ces recommandations, le fait de soumettre ce recueil à un contrôle préalable risquerait de rendre impossible la mise en œuvre desdites recommandations.

51 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 ? »

Sur les questions préjudicielles

52 Par ses trois questions préjudicielles, qu'il convient d'examiner conjointement, la juridiction de renvoi demande, en substance, si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale qui autorise l'autorité publique chargée de la protection des droits d'auteur et des droits voisins contre les atteintes à ces droits commises sur Internet à accéder aux données, conservées par les fournisseurs de services de communications électroniques accessibles au public, relatives à l'identité civile correspondant à des adresses IP collectées préalablement par des organismes d'ayants droit, afin que cette autorité publique puisse identifier les titulaires de ces adresses, utilisées pour des activités susceptibles de constituer de telles atteintes, et puisse prendre, le cas échéant, des mesures à leur égard, sans que cet accès soit subordonné à l'exigence d'un contrôle préalable par une juridiction ou une entité administrative indépendante.

Observations liminaires

53 Dans l'affaire au principal, sont en cause deux traitements de données à caractère personnel distincts et successifs qui interviennent dans le cadre des activités de la Hadopi, autorité publique indépendante, dont la mission consiste, notamment, conformément à l'article L. 331-13 du CPI, en la protection des œuvres et des

objets couverts par un droit d'auteur ou un droit voisin contre des atteintes à ces droits commises sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne.

54 Le premier traitement, effectué en amont par des agents assermentés et agréés d'organismes d'ayants droit, se déroule en deux temps. Dans un premier temps, des adresses IP qui apparaissent avoir été utilisées pour des activités susceptibles de constituer une atteinte à un droit d'auteur ou à un droit voisin sont collectées sur les réseaux de pair à pair. Dans un second temps, un ensemble de données à caractère personnel et d'informations sont mises à la disposition de la Hadopi, sous forme de procès-verbaux. Ces données sont, selon la liste figurant au point 1° de l'annexe du décret nº 2010-236, la date et l'heure des faits, l'adresse IP des abonnés concernés, le protocole pair à pair utilisé, le pseudonyme utilisé par l'abonné, les informations relatives aux œuvres ou objets protégés concernés par les faits, le nom du fichier tel que présent sur le poste de l'abonné (le cas échéant), et le fournisseur d'accès à Internet auprès duquel l'accès a été souscrit ou ayant fourni la ressource technique IP.

55 Le second traitement, effectué en aval par les fournisseurs d'accès à Internet sur demande de la Hadopi, se déroule également en deux temps. Dans un premier temps, les adresses IP collectées en amont sont mises en correspondance avec les titulaires de ces adresses. Dans un second temps, un ensemble de données à caractère personnel et d'informations relatives auxdits titulaires, portant essentiellement sur leur identité civile, sont mises à la disposition de cette autorité publique. Ces données sont, selon la liste figurant au point 2° de l'annexe du décret nº 2010-236, essentiellement, le nom de famille et les prénoms, l'adresse postale et les adresses électroniques, les coordonnées téléphoniques ainsi que l'adresse de l'installation téléphonique de l'abonné.

56 À ce dernier égard, l'article L. 331-21 du CPI prévoit, à son cinquième alinéa, dans sa version résultant de la décision du Conseil constitutionnel mentionnée au point 43 du présent arrêt, que les membres de la commission de protection des droits de la Hadopi et les agents publics assermentés de cette autorité habilités par son président peuvent 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.

57 Ces différents traitements de données à caractère personnel visent à permettre à la Hadopi de prendre, à l'égard des titulaires d'adresses IP ainsi identifiés, les mesures prévues dans le cadre de la procédure administrative dite de « réponse graduée » régie par l'article L. 331-25 du CPI. Ces mesures sont, tout d'abord, l'envoi de « recommandations », qui s'apparentent à des avertissements, ensuite, en cas de saisine de la commission des droits de la Hadopi, dans un délai d'un an suivant l'envoi d'une seconde recommandation, pour des faits pouvant constituer une réitération du manquement constaté, l'information faite à l'abonné, visée à l'article R. 331-40 du CPI, que les faits sont susceptibles de constituer l'infraction dite de « négligence caractérisée », définie à l'article R. 335-5 du CPI, contravention punie d'une amende maximale de 1 500 euros et de 3 000 euros en cas de récidive, enfin, après délibération, la saisine du ministère public de faits pouvant constituer une telle contravention ou, le cas échéant, le délit de contrefaçon visé à l'article L. 335-2 du CPI ou à l'article L. 335-4 de ce code, puni de trois ans d'emprisonnement et de 300 000 euros d'amende.

58 Cela étant, les questions que pose la juridiction de renvoi concernent uniquement le traitement en aval décrit au point 55 du présent arrêt et non le traitement en amont dont les caractéristiques essentielles ont été exposées au point 54 du même arrêt.

59 Il convient toutefois de relever que, si la collecte préalable des adresses IP par les organismes d'ayants droit concernés était contraire au droit de l'Union, ce droit s'opposerait également à l'exploitation de ces données dans le cadre du traitement subséquent par les fournisseurs de services de communications électroniques consistant à mettre en correspondance lesdites adresses avec les données relatives à l'identité civile des titulaires des mêmes adresses.

60 Dans ce contexte, il y a lieu de rappeler d'emblée que, selon la jurisprudence de la Cour, les adresses IP constituent tant des données relatives au trafic aux fins de la directive 2002/58 que des données à caractère

personnel aux fins du RGPD (voir, en ce sens, arrêt du 17 juin 2021, M.I.C.M., C-597/19, EU:C:2021:492, points 102 et 113 ainsi que jurisprudence citée).

61 Toutefois, la collecte d'adresses IP publiques et visibles par tous, par des agents d'organismes d'ayants droit, ne relève pas du champ d'application de la directive 2002/58, puisqu'un tel traitement n'intervient manifestement pas « dans le cadre de la fourniture de services de communications électroniques », au sens de l'article 3 de cette directive.

62 En revanche, une telle collecte d'adresses IP, autorisée, ainsi qu'il ressort du dossier dont dispose la Cour, dans certaines limites quantitatives et sous certaines conditions, par la Commission nationale de l'informatique et des libertés (CNIL) (France), en vue de leur transmission à la Hadopi aux fins de leur utilisation éventuelle dans des procédures administratives ou juridictionnelles ultérieures visant à lutter contre les activités portant atteinte aux droits d'auteur et aux droits voisins, constitue un « traitement », au sens de l'article 4, point 2, du RGPD, dont la licéité dépend des conditions que pose l'article 6, paragraphe 1, premier alinéa, sous f), de ce règlement, à la lumière de la jurisprudence de la Cour dégagée notamment dans les arrêts du 17 juin 2021, M.I.C.M. (C-597/19, EU:C:2021:492, points 102 et 103), ainsi que du 4 juillet 2023, Meta Platforms e.a. (Conditions générales d'utilisation d'un réseau social) (C-252/21, EU:C:2023:537, points 106 à 112 et jurisprudence citée).

63 S'agissant du traitement en aval décrit au point 55 du présent arrêt, celui-ci relève, quant à lui, du champ d'application de la directive 2002/58 puisqu'il intervient « dans le cadre de la fourniture de services de communications électroniques », au sens de l'article 3 de cette directive, pour autant que les données en cause sont obtenues auprès des fournisseurs de services de communications électroniques conformément à l'article L. 331-21 du CPI.

Sur l'existence d'une justification au titre de l'article 15, paragraphe 1, de la directive 2002/58 de l'accès d'une autorité publique à des données relatives à l'identité civile correspondant à une adresse IP conservées par les fournisseurs de services de communications électroniques aux fins de la lutte contre la contrefaçon commise en ligne

64 Au vu des observations liminaires qui précèdent, la question se pose de savoir si, ainsi que se le demande la juridiction de renvoi, la limitation des droits fondamentaux consacrés aux articles 7, 8 et 11 de la Charte que comporte l'accès par une autorité publique, telle que la Hadopi, à des données relatives à l'identité civile correspondant à une adresse IP dont elle dispose déjà est susceptible d'être justifiée au titre de l'article 15, paragraphe 1, de la directive 2002/58.

65 Or, l'accès à de telles données à caractère personnel ne peut être octroyé que pour autant que celles-ci ont été conservées conformément à la directive 2002/58 [voir, en ce sens, arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 29].

Sur les exigences entourant la conservation des données relatives à l'identité civile et des adresses IP correspondantes par les fournisseurs de services de communications électroniques

66 L'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive, lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par l'un de ces motifs. Cela étant, la faculté de déroger aux droits et aux obligations prévus aux articles 5, 6 et 9 de la directive 2002/58 ne saurait justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et, en particulier, à l'interdiction de stocker ces données, explicitement prévue à l'article 5 de cette

directive, devienne la règle (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 110 et 111).

67 Une mesure législative adoptée au titre de cette disposition doit, partant, répondre effectivement et strictement à l'un des objectifs mentionnés au point précédent, l'énumération de ceux-ci à l'article 15, paragraphe 1, première phrase, de la directive 2002/58 présentant un caractère exhaustif, et respecter les principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte. À cet égard, la Cour a déjà jugé que l'obligation imposée par un État membre aux fournisseurs de services de communications électroniques, par une réglementation nationale, de conserver les données relatives au trafic afin de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, relatifs, respectivement, à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel, mais également de l'article 11 de la Charte, relatif à la liberté d'expression (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 112 et 113).

68 Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 doit tenir compte de l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour, ainsi que du droit à la liberté d'expression, ce droit fondamental, garanti à l'article 11 de la Charte, constituant l'un des fondements essentiels d'une société démocratique et pluraliste et faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 114 ainsi que jurisprudence citée).

69 Il y a lieu de souligner, à cet égard, que la conservation des données relatives au trafic et des données de localisation constitue, par elle-même, d'une part, une dérogation à l'interdiction, prévue à l'article 5, paragraphe 1, de la directive 2002/58, faite à toute autre personne que les utilisateurs de stocker ces données et, d'autre part, une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte, sans qu'il importe de savoir si les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence. Il est également sans pertinence que les données conservées soient ou non utilisées par la suite, l'accès à de telles données constituant, quelle que soit l'utilisation qui en est faite ultérieurement, une ingérence distincte dans les droits fondamentaux visés au point précédent (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 115 et 116).

70 Cela étant, en ce qu'il permet aux États membres d'introduire certaines mesures dérogatoires, ainsi qu'il a été rappelé au point 66 du présent arrêt, l'article 15, paragraphe 1, de la directive 2002/58 reflète la circonstance que les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société. En effet, ainsi qu'il ressort de l'article 52, paragraphe 1, de la Charte, celle-ci admet des limitations à l'exercice de ces droits, pour autant que ces limitations sont prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 120 et 121).

71 En l'occurrence, il y a lieu de relever que, si, formellement, la Hadopi est autorisée à accéder seulement aux données relatives à l'identité civile correspondant à une adresse IP, cet accès présente la particularité qu'il nécessite, au préalable, une mise en correspondance entre l'adresse IP et les données d'identité civile de son titulaire par les fournisseurs de services de communications électroniques concernés. Ledit accès présuppose donc nécessairement que les fournisseurs disposent des adresses IP de même que des données relatives à l'identité de leurs titulaires.

72 En outre, cette autorité publique cherche à obtenir l'accès à ces données dans le seul but d'identifier le titulaire d'une adresse IP ayant été utilisée pour des activités susceptibles de porter atteinte aux droits d'auteur ou

aux droits voisins, dès lors qu'il a illégalement mis à disposition sur Internet des œuvres protégées, en vue d'un téléchargement de celles-ci par d'autres personnes. Dans ces conditions, les données relatives à l'identité civile doivent être considérées comme étant étroitement liées tant à l'adresse IP qu'aux informations relatives à l'œuvre mise à disposition sur Internet dont dispose la Hadopi.

73 Or, il ne saurait être fait abstraction d'un tel contexte particulier dans le cadre de l'examen de l'éventuelle justification d'une mesure de conservation de données à caractère personnel au titre de l'article 15, paragraphe 1, de la directive 2002/58, interprété à la lumière des articles 7, 8 et 11 de la Charte (voir, par analogie, Cour EDH, 24 avril 2018, Benedik c. Slovénie, CE:ECHR:2018:0424JUD006235714, § 109).

74 Partant, c'est au regard des exigences découlant, en matière de conservation d'adresses IP, dudit article 15, paragraphe 1, interprété à la lumière des articles 7, 8 et 11 de la Charte, qu'il convient d'examiner une éventuelle justification de l'ingérence dans les droits fondamentaux consacrés par ces derniers articles de la Charte que comporte la conservation, par les fournisseurs de services de communications électroniques accessibles au public, des données auxquelles la Hadopi a un pouvoir d'accès.

75 Dans ce contexte, il y a lieu de relever que, selon la jurisprudence de la Cour, si, ainsi qu'il a été rappelé au point 60 du présent arrêt, les adresses IP constituent des données relatives au trafic aux fins de la directive 2002/58, ces adresses se distinguent des autres catégories de données relatives au trafic ainsi que des données de localisation.

76 À cet égard, la Cour a relevé que les adresses IP sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, le propriétaire d'un équipement terminal à partir duquel une communication au moyen d'Internet est effectuée. Ainsi, en matière de courrier électronique et de téléphonie par Internet, pour autant que seules les adresses IP de la source de la communication sont conservées et non celles du destinataire de celle-ci, ces adresses ne révèlent, en tant que telles, aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication. Dans cette mesure, cette catégorie de données présente un degré de sensibilité moindre que les autres données relatives au trafic (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 152).

77 Certes, au point 156 de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), la Cour a jugé que, en dépit du constat d'une moindre sensibilité des adresses IP lorsqu'elles servent exclusivement à identifier l'utilisateur d'un service de communications électroniques, l'article 15, paragraphe 1, de la directive 2002/58 s'oppose à ce qu'une conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion soit effectuée pour des objectifs autres que la lutte contre la criminalité grave, la prévention des menaces graves contre la sécurité publique ou la sauvegarde de la sécurité nationale. Toutefois, la Cour s'est expressément fondée, pour parvenir à cette conclusion, sur le caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7, 8 et 11 de la Charte qu'est susceptible de comporter une telle conservation des adresses IP.

78 En effet, la Cour a considéré, au point 153 du même arrêt, que, dans la mesure où les adresses IP peuvent, notamment, lorsqu'elles sont utilisées pour effectuer le « traçage exhaustif du parcours de navigation d'un internaute » et, par suite, de son activité en ligne, permettre d'établir le « profil détaillé » de ce dernier, la conservation et l'analyse desdites adresses IP que nécessite un tel traçage constituent des ingérences graves dans les droits fondamentaux de la personne concernée consacrés aux articles 7 et 8 de la Charte, pouvant également avoir des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression garantie à l'article 11 de la Charte.

79 Toutefois, il y a lieu de souligner que toute conservation généralisée et indifférenciée d'un ensemble, le cas échéant vaste, d'adresses IP statiques et dynamiques utilisées par une personne dans une période donnée ne constitue pas nécessairement une ingérence grave dans les droits fondamentaux garantis aux articles 7, 8 et 11 de la Charte.

80 À cet égard, tout d'abord, les affaires ayant donné lieu à l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), portaient sur des réglementations nationales qui

impliquaient une obligation de conservation d'un ensemble de données nécessaires pour déterminer la date, l'heure, la durée et le type de la communication, identifier le matériel de communication utilisé ainsi que localiser les équipements terminaux et les communications, données au nombre desquelles figuraient, notamment, le nom et l'adresse de l'utilisateur, les numéros de téléphone de l'appelant et de l'appelé ainsi que l'adresse IP pour les services Internet. De surcroît, dans deux de ces affaires, les réglementations nationales en cause semblaient couvrir également les données relatives à l'acheminement des communications électroniques par les réseaux, celles-ci permettant également d'identifier la nature des informations consultées en ligne (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 82 et 83).

81 La conservation des adresses IP opérée dans le cadre de telles réglementations nationales était donc de nature, au regard des autres données dont ces réglementations imposaient la conservation et de la possibilité de combiner ces différentes données, à permettre de tirer des conclusions précises sur la vie privée des personnes dont les données étaient concernées et, partant, de conduire à une ingérence grave dans les droits fondamentaux, consacrés aux articles 7 et 8 de la Charte, relatifs à la protection de la vie privée et des données à caractère personnel de ces personnes, ainsi qu'à l'article 11 de cette charte, relatif à la liberté d'expression de celles-ci.

82 En revanche, l'obligation faite aux fournisseurs de services de communications électroniques, par une mesure législative au titre de l'article 15, paragraphe 1, de la directive 2002/58, d'assurer la conservation généralisée et indifférenciée des adresses IP peut, le cas échéant, être justifiée par l'objectif de la lutte contre les infractions pénales en général lorsqu'il est effectivement exclu que cette conservation puisse engendrer des ingérences graves dans la vie privée de la personne concernée en raison de la possibilité de tirer des conclusions précises sur celle-ci moyennant, notamment, une mise en relation de ces adresses IP avec un ensemble de données de trafic ou de localisation qui auraient également été conservées par ces fournisseurs.

83 Partant, un État membre qui entend imposer aux fournisseurs de services de communications électroniques une obligation de conservation généralisée et indifférenciée des adresses IP en vue d'atteindre un objectif lié à la lutte contre les infractions pénales en général doit s'assurer que les modalités de conservation de ces données soient de nature à garantir qu'est exclue toute combinaison desdites adresses IP avec d'autres données conservées, dans le respect de la directive 2002/58, qui permettrait de tirer des conclusions précises sur la vie privée des personnes dont les données seraient ainsi conservées.

84 Afin d'assurer que soit exclue une telle combinaison de données permettant de tirer des conclusions précises sur la vie privée de la personne en cause, les modalités de conservation doivent concerner la structure même de la conservation qui, en substance, doit être organisée de manière à garantir une séparation effectivement étanche des différentes catégories de données conservées.

85 À cet égard, il appartient certes à l'État membre qui entend imposer aux fournisseurs de services de communications électroniques une obligation de conservation généralisée et indifférenciée des adresses IP en vue d'atteindre un objectif lié à la lutte contre les infractions pénales en général de prévoir, dans sa législation, des règles claires et précises relatives auxdites modalités de conservation, ces modalités devant répondre à des exigences strictes. La Cour peut toutefois fournir des précisions relatives à ces modalités.

86 En premier lieu, les règles nationales mentionnées au point précédent doivent assurer que chaque catégorie de données, y compris les données relatives à l'identité civile et les adresses IP, est conservée de manière pleinement séparée des autres catégories de données conservées.

87 En deuxième lieu, ces règles doivent garantir que, sur un plan technique, la séparation des différentes catégories de données conservées, notamment les données relatives à l'identité civile, les adresses IP, les différentes données relatives au trafic autres que les adresses IP et les différentes données de localisation, est effectivement étanche, moyennant un dispositif informatique sécurisé et fiable.

88 En troisième lieu, en tant que lesdites règles prévoient la possibilité d'une mise en relation des adresses IP conservées avec l'identité civile de la personne concernée dans le respect des exigences découlant de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 de la Charte, elles ne

doivent permettre une telle mise en relation que par l'usage d'un procédé technique performant ne remettant pas en cause l'efficacité de la séparation étanche de ces catégories de données.

89 En quatrième lieu, la fiabilité de cette séparation étanche doit faire l'objet d'un contrôle régulier par une autorité publique autre que celle qui cherche à obtenir l'accès aux données à caractère personnel conservées par les fournisseurs de services de communications électroniques

90 Pour autant que sont prévues, dans la législation nationale applicable, de telles exigences strictes relatives aux modalités de conservation généralisée et indifférenciée des adresses IP et des autres données conservées par les fournisseurs de services de communications électroniques, l'ingérence résultant de cette conservation des adresses IP ne saurait, en raison de la structure même de ladite conservation, être qualifiée de « grave ».

91 En effet, dans le cas où un tel dispositif législatif est institué, les modalités de conservation des adresses IP ainsi prescrites excluent que ces données puissent être combinées avec d'autres données conservées dans le respect de la directive 2002/58, permettant de tirer des conclusions précises sur la vie privée de la personne concernée.

92 Par conséquent, en présence d'un dispositif législatif répondant aux exigences exposées aux points 86 à 89 du présent arrêt, garantissant qu'aucune combinaison de données ne permettra de tirer des conclusions précises sur la vie privée de la personne en cause, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 de la Charte, ne s'oppose pas à ce que l'État membre concerné impose une obligation de conservation généralisée et indifférenciée des adresses IP aux fins d'un objectif de lutte contre les infractions pénales en général.

93 Enfin, un tel dispositif législatif doit, ainsi qu'il ressort du point 168 de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), prévoir une durée de conservation limitée au strict nécessaire et assurer, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus ainsi que contre tout accès à ces données et toute utilisation illicites de celles-ci.

94 Il appartient à la juridiction de renvoi de vérifier si la réglementation nationale en cause au principal respecte les exigences rappelées aux points 85 à 93 du présent arrêt.

Sur les exigences entourant l'accès aux données relatives à l'identité civile correspondant à une adresse IP conservées par les fournisseurs de services de communications électroniques

95 Il découle de la jurisprudence de la Cour que, dans le domaine de la lutte contre les infractions pénales, seuls les objectifs de lutte contre la criminalité grave ou de prévention de menaces graves pour la sécurité publique sont de nature à justifier l'ingérence grave dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte l'accès des autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, 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 permettant de tirer des conclusions précises sur la vie privée des personnes concernées, sans que d'autres facteurs tenant à la proportionnalité d'une demande d'accès, tels que la durée de la période pour laquelle l'accès est sollicité à de telles données, puissent avoir pour effet que l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général soit susceptible de justifier un tel accès [arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 35].

96 En revanche, lorsque l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte l'accès des autorités publiques aux données relatives à l'identité civile conservées par les fournisseurs de services de communications électroniques, sans que ces données puissent être associées à des informations relatives aux communications effectuées, n'est pas grave dès lors que, prises dans leur ensemble, ces données ne permettent pas de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées, ledit accès est susceptible d'être justifié par un objectif de

prévention, de recherche, de détection et de poursuite des infractions pénales en général (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 54, 57 et 60).

97 Il importe également d'ajouter que, selon un principe consacré par une jurisprudence constante de la Cour, l'accès à des données de trafic et à des données de localisation ne peut être justifié en vertu de l'article 15, paragraphe 1, de la directive 2002/58 que par l'objectif d'intérêt général pour lequel leur conservation a été imposée aux fournisseurs de services de communications électroniques, sauf si cet accès est justifié par un objectif d'intérêt général de plus grande importance. Il découle notamment de ce principe qu'un tel accès à des fins de lutte contre les infractions en général ne saurait en aucun cas être accordé lorsque la conservation desdites données a été justifiée par l'objectif de lutte contre la criminalité grave ou, a fortiori, de sauvegarde de la sécurité nationale (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 166).

98 En revanche, un tel objectif de lutte contre les infractions pénales en général permet de justifier qu'il soit donné accès aux données de trafic et de localisation qui ont été stockées et donc conservées dans la mesure et pour la durée nécessaires à la commercialisation des services, à la facturation et à la fourniture de services à valeur ajoutée, comme l'autorise l'article 6 de la directive 2002/58 (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 108 et 167).

99 En l'occurrence, en premier lieu, il ressort de la réglementation nationale en cause au principal que la Hadopi n'a pas accès à un « ensemble de données relatives au trafic ou de données de localisation », au sens de la jurisprudence rappelée au point 95 du présent arrêt, de sorte qu'elle ne peut pas, en principe, tirer des conclusions précises sur la vie privée des personnes concernées. Or, un accès qui ne permet pas de tirer de telles conclusions ne constitue pas une ingérence grave dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte.

100 En effet, selon cette réglementation et les explications fournies par le gouvernement français à ce sujet, l'accès accordé à cette autorité publique est strictement limité à certaines données relatives à l'identité civile du titulaire d'une adresse IP et est autorisé à seule fin de pouvoir identifier ce titulaire soupçonné de s'être livré à une activité portant atteinte aux droits d'auteur ou aux droits voisins dès lors qu'il a illégalement mis à disposition sur Internet des œuvres protégées, en vue d'un téléchargement de celles-ci par d'autres personnes. Cet accès vise, le cas échéant, à l'adoption à l'égard de ce titulaire de l'une des mesures pédagogiques ou répressives prévues dans le cadre de la procédure de réponse graduée, à savoir l'envoi d'une première et d'une seconde recommandation puis d'une lettre lui notifiant que cette activité est susceptible de constituer l'infraction de négligence caractérisée et, enfin, la saisine du ministère public aux fins de la poursuite de cette contravention ou du délit de contrefaçon.

101 Encore faut-il que ladite réglementation nationale prévoie des règles claires et précises de nature à assurer que les adresses IP conservées dans le respect de la directive 2002/58 puissent uniquement être utilisées pour identifier la personne à laquelle une adresse IP déterminée a été attribuée, tout en excluant une utilisation permettant de surveiller, au moyen d'une ou de plusieurs de ces adresses, l'activité en ligne de cette personne. Lorsqu'une adresse IP est ainsi utilisée à seule fin d'identifier son titulaire dans le cadre d'une procédure administrative spécifique pouvant déboucher sur des poursuites pénales contre celui-ci et non à des fins visant, par exemple, à révéler les contacts ou la localisation de ce titulaire, l'accès à cette adresse à cette seule fin concerne ladite adresse en tant que donnée relative à l'identité civile plutôt qu'en tant que donnée relative au trafic.

102 De plus, il découle du principe consacré par la jurisprudence constante rappelée au point 97 du présent arrêt qu'un accès tel que celui dont bénéficie la Hadopi en vertu de la réglementation nationale en cause au principal, dès lors qu'il poursuit l'objectif de la lutte contre les infractions pénales en général, ne saurait être justifié que s'il porte sur des adresses IP qui doivent être conservées par les fournisseurs de services de communications électroniques aux fins de cet objectif et non aux fins d'un objectif de plus grande importance tel que celui de la lutte contre la criminalité grave, sans préjudice toutefois d'un accès justifié par un tel objectif de lutte contre les infractions en général lorsqu'il porte sur des adresses IP stockées et donc conservées dans les conditions prévues à l'article 6 de la directive 2002/58.

103 En outre, ainsi qu'il ressort des points 85 à 92 du présent arrêt, la conservation d'adresses IP, fondée sur une mesure législative au titre de l'article 15, paragraphe 1, de la directive 2002/58, aux fins de l'objectif de la lutte contre les infractions pénales en général, peut être justifiée lorsque les modalités de cette conservation instituées par le dispositif législatif concerné répondent à un ensemble d'exigences visant à assurer, en substance, une séparation effectivement étanche des différentes catégories de données conservées, de telle sorte que la combinaison de données appartenant à différentes catégories est effectivement exclue. En effet, dans le cas où de telles modalités de conservation sont imposées aux fournisseurs de services de communications électroniques, une conservation généralisée et indifférenciée des adresses IP ne constitue pas une ingérence grave dans la vie privée de leurs titulaires puisque ces données ne permettent pas de tirer des conclusions précises sur leur vie privée.

104 Partant, eu égard à la jurisprudence rappelée aux points 95 à 97 du présent arrêt, dans le cas où un tel dispositif législatif est mis en place, l'accès aux adresses IP conservées aux fins de l'objectif de la lutte contre les infractions pénales en général peut être justifié au regard de l'article 15, paragraphe 1, de la directive 2002/58 lorsque cet accès est autorisé à seule fin d'identifier la personne soupçonnée d'être impliquée dans de telles infractions.

105 Au demeurant, permettre à une autorité publique telle que la Hadopi d'avoir accès à des données relatives à l'identité civile correspondant à une adresse IP publique qui lui a été transmise par des organismes d'ayants droit à seule fin d'identifier le titulaire de cette adresse utilisée pour des activités commises en ligne et susceptibles de porter atteinte aux droits d'auteur ou aux droits voisins, en vue de l'imposition à son égard de l'une des mesures prévues dans le cadre de la procédure de réponse graduée, est conforme à la jurisprudence de la Cour concernant le « droit d'information » dans le contexte d'une action relative à une atteinte à un droit de propriété intellectuelle telle que prévue à l'article 8 de la directive 2004/48 (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, points 47 et suivants).

106 En effet, dans le cadre de cette jurisprudence, tout en soulignant que l'application des mesures prévues par la directive 2004/48 ne saurait affecter le RGPD ni la directive 2002/58, la Cour a jugé que l'article 8, paragraphe 3, de la directive 2004/48, lu en combinaison avec l'article 15, paragraphe 1, de la directive 2002/58 et l'article 7, sous f), de la directive 95/46, ne s'oppose pas à ce que les États membres établissent à la charge des fournisseurs de services de communications électroniques 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, mais n'impose pas non plus à ces États de prévoir une telle obligation (voir, en ce sens, arrêt du 17 juin 2021, M.I.C.M., C-597/19, EU:C:2021:492, points 124 et 125 ainsi que jurisprudence citée).

107 Cela étant, en second lieu, aux fins de l'appréciation concrète du degré de l'ingérence dans la vie privée que comporte un accès d'une autorité publique à des données à caractère personnel, il ne saurait être fait abstraction des spécificités du contexte dans lequel cet accès a lieu et, en particulier, de l'ensemble des données et des informations communiquées à cette autorité en vertu de la réglementation nationale applicable, y compris des données et des informations préexistantes révélatrices du contenu (voir, par analogie, Cour EDH, 24 avril 2018, Benedik c. Slovénie, CE:ECHR:2018:0424JUD006235714, § 109).

108 Ainsi, en l'occurrence, il importe de tenir compte, aux fins de ladite appréciation, du fait que, antérieurement à l'accès aux données relatives à l'identité civile en cause dont elle bénéficie, la Hadopi est destinataire de la part des organismes d'ayants droit, notamment, des « informations relatives aux œuvres ou objets protégés concernés par les faits » et, « le cas échéant », du « nom du fichier tel que présent sur le poste de l'abonné », conformément au point 1° de l'annexe du décret nº 2010-236.

109 Il ressort du dossier dont dispose la Cour, mais sous réserve de vérification par la juridiction de renvoi, que les informations sur l'œuvre concernée, telles que consignées dans un procès-verbal dont le contenu est encadré par les délibérations de la CNIL du 10 juin 2010 se limitent, essentiellement, au titre de l'œuvre concernée ainsi qu'à un extrait dénommé « chunk », se présentant sous la forme d'une suite alphanumérique et non d'une captation audio ou vidéo de l'œuvre.

110 À cet égard, certes, il ne saurait, de manière générale, être exclu que l'accès d'une autorité publique à un nombre limité de données relatives à l'identité civile du titulaire d'une adresse IP qui lui a été communiquée

par un fournisseur de services de communications électroniques à seule fin d'identifier ce titulaire dans le cas où cette adresse a été utilisée pour des activités susceptibles de porter atteinte aux droits d'auteur ou aux droits voisins, s'il est combiné avec l'analyse d'informations, même limitées, sur le contenu de l'œuvre illégalement mise à disposition sur Internet qui lui ont été transmises antérieurement par les organismes d'ayants droit, soit susceptible de renseigner cette autorité publique sur certains aspects de la vie privée dudit titulaire, y compris sur des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé, alors que de telles données jouissent, par ailleurs, d'une protection particulière dans le droit de l'Union.

111 Toutefois, en l'occurrence, au vu de la nature des données et des informations limitées dont dispose la Hadopi, ce n'est que dans des situations atypiques que celles-ci seraient susceptibles de révéler des informations, le cas échéant sensibles, sur des aspects de la vie privée de la personne en cause qui, prises ensemble, pourraient permettre à cette autorité publique de tirer des conclusions précises sur la vie privée de celle-ci, par exemple en établissant son profil détaillé.

112 Tel pourrait notamment être le cas d'une personne dont l'adresse IP a été utilisée pour des activités portant atteinte aux droits d'auteur ou aux droits voisins sur des réseaux de pair à pair de manière répétée, voire à grande échelle, en lien avec des œuvres protégées de types particuliers pouvant être regroupées sur la base des termes de leur titre qui sont susceptibles de révéler des informations, le cas échéant sensibles, sur des aspects de sa vie privée.

113 Cela étant, divers éléments permettent de considérer que, en l'occurrence, l'ingérence dans la vie privée d'une personne soupçonnée de s'être livrée à une activité portant atteinte aux droits d'auteur ou aux droits voisins que permet une réglementation telle que celle en cause au principal ne revêt pas nécessairement un degré de gravité élevé. Tout d'abord, conformément à une telle réglementation, l'accès de la Hadopi aux données à caractère personnel en cause est réservé à un nombre limité d'agents agréés et assermentés de cette autorité publique, organe qui bénéficie d'ailleurs d'un statut indépendant conformément à l'article L. 331-12 du CPI. Ensuite, cet accès a pour but unique d'identifier une personne soupçonnée de s'être livrée à une activité portant atteinte aux droits d'auteur ou aux droits voisins lorsqu'il est constaté qu'une œuvre protégée a illégalement été mise à disposition à partir de son accès à Internet. Enfin, l'accès de la Hadopi aux données à caractère personnel en cause est strictement limité aux données nécessaires à cette fin (voir, par analogie, Cour EDH, 17 octobre 2019, López Ribalda e.a. c. Espagne, CE:ECHR:2019:1017JUD000187413, § 126 et 127).

114 Un autre élément de nature à réduire encore davantage le degré d'ingérence dans les droits fondamentaux à la protection de la vie privée et des données à caractère personnel découlant dudit accès de la Hadopi, qui semble ressortir du dossier dont dispose la Cour mais qu'il incombe à la juridiction de renvoi de vérifier, concerne le fait que, en vertu de la réglementation nationale applicable, les agents de la Hadopi ayant accès aux données et aux informations concernées sont tenus à une obligation de confidentialité leur interdisant de les divulguer sous quelque forme que ce soit, sauf à seules fins de saisir le ministère public, et d'utiliser celles-ci à des fins autres que l'identification du titulaire d'une adresse IP soupçonné de s'être livré à une activité portant atteinte au droit d'auteur ou à un droit voisin afin de lui imposer l'une des mesures prévues dans le cadre de la procédure de réponse graduée (voir, par analogie, Cour EDH, 17 décembre 2009, Gardel c. France, CE:ECHR:2009:1217JUD001642805, § 70).

115 Ainsi, pour autant qu'une réglementation nationale satisfasse aux conditions rappelées au point 101 du présent arrêt, les adresses IP communiquées à une autorité publique telle que la Hadopi ne permettent pas de procéder au traçage du parcours de navigation de leur titulaire, ce qui tend à confirmer le constat selon lequel l'ingérence que comporte l'accès de cette autorité aux données d'identification en cause au principal ne saurait être qualifiée de grave.

116 En troisième lieu, il y a lieu de rappeler que, aux fins de la conciliation nécessaire des droits et des intérêts en cause qu'impose l'exigence de proportionnalité prescrite à l'article 15, paragraphe 1, première phrase, de la directive 2002/58, même si la liberté d'expression et la confidentialité des données à caractère personnel sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services Internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, ces droits fondamentaux ne sont pas pour autant absolus. En effet, dans le cadre d'une mise en balance des droits et intérêts en cause, ceux-ci doivent parfois s'effacer devant d'autres droits fondamentaux et des impératifs d'intérêt général tels

que la défense de l'ordre public et la prévention des infractions pénales ou la protection des droits et libertés d'autrui. Tel est, en particulier, le cas lorsque la prépondérance accordée auxdites préoccupations primordiales est de nature à entraver l'efficacité d'une enquête pénale, notamment en rendant impossible ou excessivement difficiles l'identification effective de l'auteur d'une infraction pénale et l'imposition d'une sanction à son égard (voir, par analogie, Cour EDH, 2 mars 2009, K.U. c. Finlande, CE:ECHR:2008:1202JUD000287202, § 49).

117 Dans ce contexte, il doit être dûment tenu compte du fait que, comme la Cour l'a déjà jugé, s'agissant d'infractions commises en ligne, l'accès aux adresses IP peut constituer le seul moyen d'investigation permettant l'identification effective de la personne à laquelle cette adresse était attribuée au moment de la commission de l'infraction (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 154).

118 Cette circonstance tend à établir, comme l'a également relevé, en substance, M. l'avocat général au point 59 de ses conclusions du 28 septembre 2023, que la conservation de ces adresses et l'accès à celles-ci sont, s'agissant de la lutte contre des infractions pénales telles que celles portant atteinte aux droits d'auteur ou aux droits voisins commises en ligne, strictement nécessaires à la réalisation de l'objectif poursuivi et répondent donc à l'exigence de proportionnalité qu'impose l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière du considérant 11 de cette directive ainsi que de l'article 52, paragraphe 2, de la Charte.

119 Ne pas permettre un tel accès comporterait d'ailleurs, comme l'a souligné, en substance, M. l'avocat général aux points 78 à 80 de ses conclusions du 27 octobre 2022 ainsi qu'aux points 80 et 81 de ses conclusions du 28 septembre 2023, un réel risque d'impunité systémique non seulement d'infractions pénales portant atteinte aux droits d'auteur ou aux droits voisins, mais également d'autres types d'infractions pénales commises en ligne ou dont la commission ou la préparation est facilitée par les caractéristiques propres à Internet. Or, l'existence d'un tel risque constitue une circonstance pertinente afin d'apprécier, dans le cadre d'une mise en balance des différents droits et intérêts en présence, si une ingérence dans les droits garantis aux articles 7, 8 et 11 de la Charte est une mesure proportionnée au regard de l'objectif de lutte contre les infractions pénales.

120 Il est vrai que l'accès d'une autorité publique telle que la Hadopi à des données d'identité civile correspondant à l'adresse IP à partir de laquelle a été commise l'infraction en ligne n'est pas nécessairement l'unique moyen d'investigation possible afin d'identifier la personne titulaire de cette adresse au moment de la commission de cette infraction. En effet, une telle identification pourrait également être a priori possible en examinant l'ensemble des activités en ligne de la personne concernée, notamment en analysant les « traces » que celle-ci aurait pu laisser sur les réseaux sociaux, tels l'identifiant utilisé sur ces réseaux ou ses coordonnées.

121 Toutefois, comme l'a relevé M. l'avocat général au point 83 de ses conclusions du 28 septembre 2023, un tel moyen d'investigation serait particulièrement intrusif puisqu'il serait susceptible de révéler des informations précises sur la vie privée des personnes concernées. Il impliquerait ainsi, pour ces personnes, une ingérence dans les droits garantis aux articles 7, 8 et 11 de la Charte plus grave que celle découlant d'une réglementation telle que celle en cause au principal.

122 Il découle de ce qui précède 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, en principe, à une réglementation nationale permettant l'accès, par une autorité publique chargée de la protection des droits d'auteur et des droits voisins contre des atteintes à ces droits commises sur Internet, à des données relatives à l'identité civile correspondant à des adresses IP collectées préalablement par des organismes d'ayants droit et conservées par les fournisseurs de services de communications électroniques de manière séparée et effectivement étanche, à seule fin 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. Dans un tel cas, la réglementation nationale applicable doit interdire aux agents disposant d'un tel accès, premièrement, de divulguer sous quelque forme que ce soit des informations sur le contenu des fichiers consultés par ces titulaires sauf à seules fins de saisir le ministère public, deuxièmement, d'effectuer tout traçage du parcours de navigation de ces titulaires et, troisièmement, d'utiliser ces adresses IP à des fins autres que celle de l'adoption de ces mesures.

Sur l'exigence d'un contrôle par une juridiction ou une entité administrative indépendante préalablement à l'accès par une autorité publique à des données relatives à l'identité civile correspondant à une adresse IP

123 La question se pose toutefois de savoir si l'accès de l'autorité publique à des données relatives à l'identité civile correspondant à une adresse IP doit être subordonné, en outre, à un contrôle préalable par une juridiction ou par une entité administrative indépendante.

124 À cet égard, c'est pour garantir, en pratique, le plein respect des conditions que les États membres sont tenus de prévoir afin d'assurer que l'accès soit limité au strict nécessaire que la Cour a jugé qu'il est « essentiel » que l'accès des autorités nationales compétentes aux données relatives au trafic et aux données de localisation soit soumis à un contrôle préalable par une juridiction ou par une entité administrative indépendante [voir, en ce sens, arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 120 ; du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 189 ; du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 51, ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 106].

125 Ce contrôle préalable requiert, premièrement, que la juridiction ou l'entité administrative indépendante chargée de l'effectuer dispose de toutes les attributions et présente toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts légitimes et des droits en cause. S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts légitimes liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 107 ainsi que jurisprudence citée).

126 Deuxièmement, lorsque ce contrôle est effectué non par une juridiction, mais par une entité administrative indépendante, celle-ci doit jouir d'un statut lui permettant d'agir lors de l'exercice de ses missions de manière objective et impartiale et doit être, à cet effet, à l'abri de toute influence extérieure. Ainsi, l'exigence d'indépendance à laquelle doit satisfaire l'entité chargée d'exercer le contrôle préalable impose que celle-ci ait la qualité de tiers par rapport à l'autorité qui demande l'accès aux données, de sorte que ladite entité soit en mesure d'exercer ce contrôle de manière objective et impartiale, en étant protégée de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité à l'égard des parties à la procédure pénale (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 108 ainsi que jurisprudence citée).

127 Troisièmement, le contrôle indépendant requis conformément à l'article 15, paragraphe 1, de la directive 2002/58 doit intervenir préalablement à tout accès aux données concernées, sauf en cas d'urgence dûment justifiée, auquel cas ledit contrôle doit intervenir dans de brefs délais. En effet, un contrôle ultérieur ne permettrait pas de répondre à l'objectif du contrôle préalable, qui consiste à empêcher que soit autorisé un accès aux données en cause qui dépasse les limites du strict nécessaire [arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 110].

128 Cela étant, si, ainsi qu'il ressort de la jurisprudence rappelée au point 124 du présent arrêt, la Cour a jugé « essentiel » que l'accès des autorités nationales compétentes aux données relatives au trafic et aux données de localisation soit soumis à un contrôle préalable par une juridiction ou par une entité administrative indépendante, cette jurisprudence s'est développée dans le contexte de mesures nationales permettant, aux fins d'un objectif lié à la lutte contre la criminalité grave, un accès général à toutes les données relatives au trafic et de localisation conservées, indépendamment d'un quelconque lien, ne serait-ce qu'indirect, avec le but poursuivi, et qui comportaient ainsi des ingérences graves et même « particulièrement graves » dans les droits fondamentaux concernés.

129 En revanche, lorsqu'étaient en cause les conditions dans lesquelles un accès aux données relatives à l'identité civile était susceptible d'être justifié au regard de l'article 15, paragraphe 1, de la directive 2002/58, lu à la

lumière des articles 7, 8 et 11 de la Charte, aucune mention explicite n'a été faite par la Cour de l'exigence d'un tel contrôle préalable [voir, en ce sens, arrêts du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 59, 60 et 62 ; du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 157 et 158, ainsi que du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 34].

130 Or, il découle de la jurisprudence de la Cour relative au principe de proportionnalité dont l'article 15, paragraphe 1, première phrase, de la directive 2002/58 impose le respect, en particulier de celle selon laquelle la possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus, notamment, aux articles 5, 6 et 9 de cette directive, doit être appréciée en mesurant la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7, 8 et 11 de la Charte 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 (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 131), que le degré d'ingérence dans les droits fondamentaux concernés que comporte l'accès aux données à caractère personnel en cause ainsi que le niveau de sensibilité de celles-ci doivent également influer sur les garanties matérielles et procédurales devant entourer cet accès, au nombre desquelles figure l'exigence d'un contrôle préalable par une juridiction ou une entité administrative indépendante.

131 Partant, eu égard à ce principe de proportionnalité, il y a lieu de considérer que l'exigence d'un contrôle préalable par une juridiction ou par une entité administrative indépendante s'impose lorsque, dans le contexte d'une réglementation nationale prévoyant l'accès d'une autorité publique à des données à caractère personnel, cet accès comporte le risque d'une ingérence grave dans les droits fondamentaux de la personne concernée en ce sens qu'il pourrait permettre à cette autorité publique de tirer des conclusions précises sur la vie privée de cette personne et, le cas échéant, d'établir son profil détaillé.

132 Inversement, cette exigence d'un contrôle préalable n'a pas vocation à s'appliquer lorsque l'ingérence dans les droits fondamentaux concernés que comporte l'accès d'une autorité publique à des données à caractère personnel ne peut être qualifiée de grave.

133 Tel est le cas de l'accès à des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques à seule fin d'identifier l'utilisateur concerné et sans que ces données puissent être associées à des informations relatives aux communications effectuées, puisque, selon la jurisprudence de la Cour, l'ingérence que comporte un tel traitement desdites données ne saurait, en principe, être qualifiée de grave (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 157 et 158).

134 Il s'ensuit que, dans le cas où un dispositif de conservation tel que celui décrit aux points 86 à 89 du présent arrêt est mis en place, l'accès de l'autorité publique aux données relatives à l'identité civile correspondant aux adresses IP ainsi conservées n'est, en principe, pas subordonné à l'exigence d'un contrôle préalable par une juridiction ou par une entité administrative indépendante.

135 Cela étant, ainsi qu'il a déjà été relevé aux points 110 et 111 du présent arrêt, il ne saurait être exclu que, dans des situations atypiques, les données et les informations limitées mises à la disposition d'une autorité publique dans le cadre d'une procédure telle que la procédure de réponse graduée en cause au principal soient susceptibles de révéler des informations, le cas échéant sensibles, sur des aspects de la vie privée de la personne concernée, informations qui, prises ensemble, pourraient permettre à cette autorité publique de tirer des conclusions précises sur la vie privée de cette personne et, le cas échéant, d'établir son profil détaillé.

136 Comme il ressort du point 112 du présent arrêt, un tel risque pour la vie privée peut se présenter, notamment, lorsqu'une personne se livre à des activités portant atteinte aux droits d'auteur ou aux droits voisins sur des réseaux de pair à pair de manière répétée, voire à grande échelle, en lien avec des œuvres protégées de types particuliers pouvant être regroupées sur la base des termes de leur titre, révélant des informations, le cas échéant sensibles, sur sa vie privée.

137 Ainsi, en l'occurrence, dans le cadre de la procédure administrative de réponse graduée, un titulaire d'une adresse IP peut être particulièrement exposé à un tel risque pour sa vie privée lorsque cette procédure atteint

le stade où la Hadopi est appelée à décider de saisir ou non le ministère public en vue de la poursuite de ce titulaire pour des faits susceptibles de constituer la contravention de négligence caractérisée ou le délit de contrefaçon.

138 En effet, cette saisine présuppose que le titulaire d'une adresse IP ait déjà fait l'objet de deux recommandations et d'une lettre de notification l'informant de ce que ses activités sont susceptibles de poursuites pénales, mesures qui impliquent que, à chaque fois, la Hadopi a eu accès à des données relatives à l'identité civile de ce titulaire dont l'adresse IP a été utilisée pour des activités portant atteinte aux droits d'auteur ou aux droits voisins ainsi qu'à un fichier relatif à cette œuvre comportant, essentiellement, son titre.

139 Or, il ne peut être exclu que, prises ensemble et au fur et à mesure que se déroule la procédure administrative de réponse graduée, les données ainsi fournies lors des différentes phases de cette procédure puissent révéler des informations concordantes et, le cas échéant, sensibles sur des aspects de la vie privée de la personne concernée permettant, le cas échéant, d'établir son profil.

140 Ainsi, l'intensité de l'atteinte au droit au respect de la vie privée est susceptible de croître au fur et à mesure que la procédure de réponse graduée, qui opère selon un processus séquentiel, parcourt les différentes étapes qui la composent.

141 En l'occurrence, l'accès de la Hadopi à l'ensemble des données relatives à la personne concernée et cumulées au cours des différentes étapes de cette procédure peut, par la mise en relation de ces données, être susceptible de permettre que soient tirées des conclusions précises sur la vie privée de celle-ci. Partant, dans le cadre d'une procédure telle que la procédure de réponse graduée en cause au principal, la réglementation nationale doit également prévoir, à un certain stade de ladite procédure, un contrôle préalable par une juridiction ou par une entité administrative indépendante, répondant aux conditions rappelées aux points 125 à 127 du présent arrêt, afin d'exclure des risques d'ingérences disproportionnées dans les droits fondamentaux à la protection de la vie privée et des données à caractère personnel de la personne concernée. Cela signifie que, en pratique, un tel contrôle doit intervenir avant que la Hadopi puisse mettre en relation des données d'identité civile d'une personne correspondant à une adresse IP et obtenues auprès d'un fournisseur de services de communications électroniques, cette personne ayant déjà fait l'objet de deux recommandations, et le fichier relatif à l'œuvre dont la mise à disposition sur Internet en vue d'un téléchargement de celle-ci par d'autres personnes. Partant, ledit contrôle doit intervenir avant l'éventuel envoi de la lettre de notification visée à l'article R-331-40 du CPI, constatant que cette personne s'est livrée à des faits pouvant constituer l'infraction de négligence caractérisée. Ce n'est qu'à la suite d'un tel contrôle préalable par une juridiction ou une autorité administrative indépendante et l'autorisation de celle-ci que la Hadopi pourra adresser une telle lettre et ensuite, le cas échéant, saisir le ministère public en vue de la poursuite de cette infraction.

142 Il convient de permettre à la Hadopi d'identifier les cas dans lesquels le titulaire de l'adresse IP concernée atteint cette troisième étape d'une telle procédure de réponse graduée. Partant, cette procédure doit être organisée et structurée de manière à ce que les données d'identité civile d'une personne correspondant à des adresses IP préalablement collectées sur Internet, recueillies auprès des fournisseurs de services de communications électroniques, ne soient pas automatiquement susceptibles d'être mises en relation, par les personnes chargées de l'examen des faits au sein de la Hadopi, avec les fichiers comportant des éléments permettant de connaître les titres des œuvres protégées dont la mise à disposition sur Internet a justifié cette collecte.

143 Ainsi, cette mise en relation aux fins de la troisième étape de la réponse graduée doit être suspendue lorsque le recueil desdites données d'identité civile, correspondant à un cas de deuxième réitération possible d'une activité portant atteinte aux droits d'auteur ou aux droits voisins, enclenche l'exigence d'un contrôle préalable par une juridiction ou par une entité administrative indépendante décrite au point 141 du présent arrêt.

144 Par ailleurs, l'aménagement de l'exigence du contrôle préalable exposé aux points 141 à 143 du présent arrêt, en ce qu'il est limité à la troisième étape de la procédure de réponse graduée et ne s'applique pas aux étapes antérieures de celle-ci, permet également de prendre en compte l'argument selon lequel il y a lieu de sauvegarder la praticabilité de cette procédure qui est caractérisée, surtout dans ses étapes antérieures à l'éventuel envoi de la lettre de notification et, le cas échéant, à la saisine du ministère public, par la nature

massive des demandes d'accès de l'autorité publique découlant du nombre tout aussi important de procès-verbaux dont elle est saisie par les organismes d'ayants droit.

145 S'agissant encore de l'objet du contrôle préalable visé aux points 141 à 143 du présent arrêt, il découle de la jurisprudence rappelée aux points 95 et 96 dudit arrêt que, dans les cas où la personne concernée est soupçonnée d'avoir commis l'infraction de « négligence caractérisée » définie à l'article R. 335-5 du CPI, relevant des infractions pénales en général, la juridiction ou l'entité administrative indépendante en charge de ce contrôle doit refuser l'accès lorsque ce dernier permettrait à l'autorité publique qui l'a sollicité de tirer des conclusions précises sur la vie privée de ladite personne.

146 En revanche, même un accès permettant de tirer de telles conclusions précises devrait être autorisé dans les cas où les éléments portés à la connaissance de cette juridiction ou de cette entité administrative indépendante permettent de soupçonner que la personne concernée a commis le délit de contrefaçon visé à l'article L. 335-2 du CPI ou à l'article L. 335-4 de ce code, étant donné qu'il est loisible pour un État membre de considérer qu'un tel délit, en tant qu'il porte atteinte à un intérêt fondamental de la société, relève des formes graves de criminalité.

147 Enfin, s'agissant des modalités de ce contrôle préalable, le gouvernement français estime que, au vu des caractéristiques particulières de l'accès par la Hadopi aux données en cause, en particulier de son caractère massif, il serait approprié qu'un contrôle préalable, s'il était requis, soit entièrement automatisé. En effet, un tel contrôle, qui présente un caractère purement objectif, viserait essentiellement à vérifier que le procès-verbal de saisine de la Hadopi contient toutes les informations et données requises sans que cette autorité soit appelée à apprécier celles-ci.

148 Toutefois, un contrôle préalable ne saurait en aucun cas être entièrement automatisé puisque, ainsi qu'il ressort de la jurisprudence rappelée au point 125 du présent arrêt, s'agissant d'une enquête pénale, un tel contrôle exige, en tout état de cause, que la juridiction ou l'entité administrative indépendante concernée soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts légitimes liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès.

149 En effet, une telle mise en balance des différents intérêts légitimes et des droits concernés nécessite l'intervention d'une personne physique, celle-ci étant d'autant plus nécessaire que l'automaticité et la grande échelle du traitement de données en cause emportent des risques pour la vie privée.

150 En outre, un contrôle entièrement automatisé n'est, en principe, pas de nature à assurer que l'accès ne dépasse pas les limites du strict nécessaire et que les personnes dont les données à caractère personnel sont concernées disposent de garanties effectives contre les risques d'abus ainsi que contre tout accès à ces données et toute utilisation illicites de celles-ci.

151 Ainsi, si des contrôles automatisés peuvent permettre de vérifier certaines des informations contenues dans les procès-verbaux des organismes d'ayants droit, de tels contrôles doivent, en tout état de cause, aller de pair avec des contrôles par des personnes physiques répondant pleinement aux exigences rappelées aux points 125 à 127 du présent arrêt.

Sur les exigences tenant aux conditions matérielles et procédurales ainsi qu'aux garanties contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données s'imposant à l'accès par une autorité publique à des données relatives à l'identité civile correspondant à une adresse IP

152 Il ressort de la jurisprudence de la Cour que l'accès à des données à caractère personnel ne saurait être conforme à l'exigence de proportionnalité qu'impose l'article 15, paragraphe 1, de la directive 2002/58 que si la mesure législative qui l'autorise prévoit, par des règles claires et précises, que ledit accès est subordonné au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'accès et d'utilisation abusifs ou illicites de ces données [voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791,

points 132 et 173, ainsi que du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 49 et jurisprudence citée].

153 Ainsi que l'a souligné la Cour, la nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé (arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 176 ainsi que jurisprudence citée).

154 À cet égard, en réponse à une question posée par la Cour en vue de l'audience du 5 juillet 2022, le gouvernement français a confirmé que, comme l'indique d'ailleurs l'article L. 331-29 du CPI, l'accès par la Hadopi aux données relatives à l'identité civile dans le cadre de la procédure de réponse graduée procède d'un traitement de données essentiellement automatisé qui s'explique par le caractère massif des contrefaçons constatées sur les réseaux de pair à pair par les organismes d'ayants droit, constatations qui sont transmises à la Hadopi sous forme de procès-verbaux.

155 Il ressort en particulier du dossier dont dispose la Cour que, lors de ce traitement de données, les agents de la Hadopi vérifient, de manière essentiellement automatisée et sans appréciation des faits concernés en tant que tels, si les procès-verbaux dont elle est saisie contiennent toutes les informations et données mentionnées au point 1° de l'annexe au décret nº 2010-236, en particulier les faits de mise à disposition illégale sur Internet concernés et les adresses IP utilisés à cette fin. Or, de tels traitements doivent aller de pair avec des contrôles par des personnes physiques.

156 Un tel traitement automatisé étant susceptible de comporter un certain nombre de faux cas positifs ainsi que et surtout le risque qu'un nombre de données à caractère personnel potentiellement très élevé soit détourné par des tiers à des fins abusives ou illicites, il importe que, en vertu d'une mesure législative, le système de traitement de données utilisé par une autorité publique fasse l'objet, à intervalles réguliers, d'un contrôle par un organisme indépendant et ayant la qualité de tiers par rapport à cette autorité, visant à vérifier l'intégrité du système, y compris les garanties effectives contre les risques d'abus ainsi que contre tout accès à ces données et toute utilisation illicites de ces dernières que ce système doit assurer ainsi que son efficacité et sa fiabilité pour détecter les manquements susceptibles d'être qualifiés, en cas de renouvellement, de négligence caractérisée ou de contrefaçon.

157 Enfin, il importe d'ajouter qu'un traitement de données à caractère personnel effectué par une autorité publique, tel que celui auquel procède la Hadopi dans le cadre de la procédure de réponse graduée, doit respecter les règles spécifiques de protection de ces données prévues par la directive 2016/680 dont l'objet est, selon son article 1er, d'établir des règles relatives 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

158 En effet, en l'occurrence, même si, en vertu du droit national applicable, elle ne dispose pas de pouvoirs décisionnels propres, la Hadopi, lorsqu'elle traite dans le cadre de la procédure de réponse graduée des données à caractère personnel et adopte des mesures telles qu'une recommandation ou l'information à la personne concernée selon laquelle les faits en cause sont passibles de poursuites pénales, doit être qualifiée d'« autorité publique », au sens de l'article 3 de la directive 2016/680, impliquée dans la prévention et la détection des infractions pénales, à savoir la contravention de négligence caractérisée ou le délit de contrefaçon, et relève donc du champ d'application de cette directive conformément à son article 1er.

159 À cet égard, le gouvernement français a indiqué, en réponse à une question posée par la Cour en vue de l'audience du 5 juillet 2022, que, les mesures adoptées par la Hadopi dans le cadre de la mise en œuvre de la procédure de réponse graduée « ayant un caractère pré-pénal directement lié à la procédure judiciaire », le système de gestion des mesures pour la protection des œuvres sur Internet, mis en œuvre par la Hadopi, est soumis, ainsi qu'il ressort de la jurisprudence de la juridiction de renvoi, aux dispositions de droit national visant à transposer la directive 2016/680.

160 En revanche, un tel traitement de données par la Hadopi ne relève pas du champ d'application du RGPD. En effet, l'article 2, paragraphe 2, sous d), du RGPD dispose que ce règlement ne s'applique pas au traitement de

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

161 Comme l'a relevé M. l'avocat général au point 104 de ses conclusions du 27 octobre 2022, le respect de la directive 2016/680 s'imposant dès lors à la Hadopi dans le cadre de la procédure de réponse graduée, les personnes impliquées dans une telle procédure doivent bénéficier d'un ensemble de garanties matérielles et procédurales englobant le droit d'accès, de rectification et d'effacement des données personnelles traitées par la Hadopi ainsi que la possibilité d'introduire une réclamation auprès d'une autorité de contrôle indépendante, suivie, le cas échéant, d'un recours juridictionnel exercé dans les conditions de droit commun.

162 Dans ce contexte, il ressort de la législation nationale en cause au principal que, dans le cadre de la procédure de réponse graduée, plus précisément lors de l'envoi de la seconde recommandation et lors de la notification subséquente que les faits constatés sont susceptibles d'être qualifiés d'infraction pénale, le destinataire de ces communications bénéficie de certaines garanties procédurales telles que le droit de présenter des observations, le droit d'obtenir des précisions sur le manquement qui lui est reproché ainsi que, s'agissant de ladite notification, le droit de solliciter une audition et de se faire assister par un conseil.

163 En tout état de cause, il appartient à la juridiction de renvoi de vérifier si cette législation nationale prévoit l'ensemble des garanties matérielles et procédurales que prescrit la directive 2016/680.

164 Eu égard à l'ensemble des considérations qui précèdent, il y a lieu de répondre aux trois 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 qui autorise l'autorité publique chargée de la protection des droits d'auteur et des droits voisins contre les atteintes à ces droits commises sur Internet à accéder aux données, conservées par les fournisseurs de services de communications électroniques accessibles au public, relatives à l'identité civile correspondant à des adresses IP collectées préalablement par des organismes d'ayants droit, afin que cette autorité puisse identifier les titulaires de ces adresses, utilisées pour des activités susceptibles de constituer de telles atteintes, et puisse prendre, le cas échéant, des mesures à leur égard, à condition que, en vertu de cette réglementation,

– ces données soient conservées dans des conditions et selon des modalités techniques garantissant qu'il soit exclu que cette conservation puisse permettre de tirer des conclusions précises sur la vie privée de ces titulaires, par exemple en établissant leur profil détaillé, ce qui peut être accompli, en particulier, en imposant aux fournisseurs de services de communications électroniques une obligation de conservation des différentes catégories de données à caractère personnel, telles les données relatives à l'identité civile, les adresses IP ainsi que les données relatives au trafic et les données de localisation, garantissant une séparation effectivement étanche de ces différentes catégories de données empêchant, au stade de la conservation, toute exploitation combinée de ces différentes catégories de données, et pour une durée ne dépassant pas le strict nécessaire,

– l'accès de cette autorité publique à de telles données conservées de manière séparée et effectivement étanche serve exclusivement à identifier la personne soupçonnée d'avoir commis une infraction pénale et soit entouré des garanties nécessaires pour exclure que, hormis dans des situations atypiques, cet accès puisse permettre de tirer des conclusions précises sur la vie privée des titulaires des adresses IP, par exemple en établissant leur profil détaillé, ce qui implique, en particulier, qu'il soit interdit aux agents de cette autorité autorisés à avoir un tel accès de divulguer, sous quelque forme que ce soit, des informations sur le contenu des fichiers consultés par ces titulaires, sauf à seules fins de saisir le ministère public, de procéder à un traçage du parcours de navigation de ces titulaires et, de manière plus générale, d'utiliser ces adresses IP à une fin autre que celle d'identifier leurs titulaires en vue de l'adoption d'éventuelles mesures contre ces derniers,

– la possibilité, pour les personnes chargées de l'examen des faits au sein de ladite autorité publique, de mettre en relation de telles données avec les fichiers comportant des éléments permettant de connaître le titre d'œuvres protégées dont la mise à disposition sur Internet a justifié la collecte des adresses IP par des organismes d'ayants droit, soit subordonnée, dans des hypothèses de nouvelle

réitération d'une activité portant atteinte aux droits d'auteur ou aux droits voisins par une même personne, à un contrôle par une juridiction ou une entité administrative indépendante, lequel ne peut être entièrement automatisé et doit intervenir préalablement à une telle mise en relation, cette dernière étant susceptible, dans de telles hypothèses, de permettre que soient tirées des conclusions précises sur la vie privée de ladite personne dont l'adresse IP a été utilisée pour des activités pouvant porter atteinte aux droits d'auteur ou aux droits voisins,

– le système de traitement de données utilisé par l'autorité publique fasse l'objet, à intervalles réguliers, d'un contrôle par un organisme indépendant et ayant la qualité de tiers par rapport à cette autorité publique visant à vérifier l'intégrité du système, y compris les garanties effectives contre les risques d'accès et d'utilisation abusifs ou illicites de ces données, ainsi que son efficacité et sa fiabilité pour détecter les éventuels manquements.

Sur les dépens

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

Par ces motifs, la Cour (assemblée plénière) dit pour droit :

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 qui autorise l'autorité publique chargée de la protection des droits d'auteur et des droits voisins contre les atteintes à ces droits commises sur Internet à accéder aux données, conservées par les fournisseurs de services de communications électroniques accessibles au public, relatives à l'identité civile correspondant à des adresses IP collectées préalablement par des organismes d'ayants droit, afin que cette autorité puisse identifier les titulaires de ces adresses, utilisées pour des activités susceptibles de constituer de telles atteintes, et puisse prendre, le cas échéant, des mesures à leur égard, à condition que, en vertu de cette réglementation,

– **ces données soient conservées dans des conditions et selon des modalités techniques garantissant qu'il soit exclu que cette conservation puisse permettre de tirer des conclusions précises sur la vie privée de ces titulaires, par exemple en établissant leur profil détaillé, ce qui peut être accompli, en particulier, en imposant aux fournisseurs de services de communications électroniques une obligation de conservation des différentes catégories de données à caractère personnel, telles les données relatives à l'identité civile, les adresses IP ainsi que les données relatives au trafic et les données de localisation, garantissant une séparation effectivement étanche de ces différentes catégories de données empêchant, au stade de la conservation, toute exploitation combinée de ces différentes catégories de données, et pour une durée ne dépassant pas le strict nécessaire,**

– **l'accès de cette autorité publique à de telles données conservées de manière séparée et effectivement étanche serve exclusivement à identifier la personne soupçonnée d'avoir commis une infraction pénale et soit entouré des garanties nécessaires pour exclure que, hormis dans des situations atypiques, cet accès puisse permettre de tirer des conclusions précises sur la vie privée des titulaires des adresses IP, par exemple en établissant leur profil détaillé, ce qui**

implique, en particulier, qu'il soit interdit aux agents de cette autorité autorisés à avoir un tel accès de divulguer, sous quelque forme que ce soit, des informations sur le contenu des fichiers consultés par ces titulaires, sauf à seules fins de saisir le ministère public, de procéder à un traçage du parcours de navigation de ces titulaires et, de manière plus générale, d'utiliser ces adresses IP à une fin autre que celle d'identifier leurs titulaires en vue de l'adoption d'éventuelles mesures contre ces derniers,

– **la possibilité, pour les personnes chargées de l'examen des faits au sein de ladite autorité publique, de mettre en relation de telles données avec les fichiers comportant des éléments permettant de connaître le titre d'œuvres protégées dont la mise à disposition sur Internet a justifié la collecte des adresses IP par des organismes d'ayants droit, soit subordonnée, dans des hypothèses de nouvelle réitération d'une activité portant atteinte aux droits d'auteur ou aux droits voisins par une même personne, à un contrôle par une juridiction ou une entité administrative indépendante, lequel ne peut être entièrement automatisé et doit intervenir préalablement à une telle mise en relation, cette dernière étant susceptible, dans de telles hypothèses, de permettre que soient tirées des conclusions précises sur la vie privée de ladite personne dont l'adresse IP a été utilisée pour des activités pouvant porter atteinte aux droits d'auteur ou aux droits voisins,**

– **le système de traitement de données utilisé par l'autorité publique fasse l'objet, à intervalles réguliers, d'un contrôle par un organisme indépendant et ayant la qualité de tiers par rapport à cette autorité publique visant à vérifier l'intégrité du système, y compris les garanties effectives contre les risques d'accès et d'utilisation abusifs ou illicites de ces données, ainsi que son efficacité et sa fiabilité pour détecter les éventuels manquements.**

Lenaerts	Bay Larsen	Arabadjiev
Prechal	Jürimäe	Lycourgos
Regan	von Danwitz	Biltgen
Piçarra	Csehi	Ilešič
Bonichot	Rodin	Xuereb
Rossi	Jarukaitis	Kumin
Jääskinen	Wahl	Ziemele
Passer	Gratsias	Arastey Sahún

Gavalec

Ainsi prononcé en audience publique à Luxembourg, le 30 avril 2024.

Le greffier — Le président

A. Calot Escobar