Provisional text

JUDGMENT OF THE COURT (Full Court)

30 April 2024 (*)

Table of Contents

Legal context
European Union law
General rules concerning the protection of personal data
– Directive 95/46/EC
– The GDPR
Sector-specific rules concerning the protection of personal data
– Directive 2002/58
– Directive (EU) 2016/680
Rules concerning the protection of intellectual property
French law
The CPI
Decree No 2010-236
The Post and Electronic Communications Code

The dispute in the main proceedings and the questions referred for a preliminary ruling

Consideration of the questions referred
Preliminary observations
Whether access by a public authority to data relating to the civil identity associated with an IP address retained by providers of electronic communications services for the purpose of combating counterfeiting offences committed online can be justified under Article 15(1) of Directive 2002/58
The requirements surrounding the retention of data relating to civil identity and associated IP addresses by providers of electronic communications services
The requirements surrounding access to data relating to the civil identity associated with an IP address retained by providers of electronic communications services
The requirement of a prior review by a court or an independent administrative body before a public authority accesses data relating to the civil identity associated with an IP address
The requirements relating to the substantive and procedural conditions and to the safeguards against the risks of abuse and against any unlawful access to and use of those data applicable to the access by a public authority to data relating to the civil identity associated with an IP address

Costs

(Reference for a preliminary ruling – Processing of personal data and the protection of privacy in the electronic communications sector – Directive 2002/58/EC – Confidentiality of electronic communications – Protection – Article 5 and Article 15(1) – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 11 and Article 52(1) – National legislation aimed at combating, through action by a public authority, counterfeiting offences committed on the internet – ‘Graduated response’ procedure – Upstream collection by rightholder organisations of IP addresses used for activities infringing copyright or related rights – Downstream access by the public authority responsible for the protection of copyright and related rights to data relating to the civil identity associated with those IP addresses retained by providers of electronic communications services – Automated processing – Requirement of prior review by a court or an independent administrative body – Substantive and procedural conditions – Safeguards against the risks of abuse and against any unlawful access to or use of those data)

In Case C-470/21,

REQUEST for a preliminary ruling under Article 267 TFEU from the Conseil d'État (Council of State, France), made by decision of 5 July 2021, received at the Court on 30 July 2021, in the proceedings

La Quadrature du Net,

Fédération des fournisseurs d'accès à Internet associatifs,

Franciliens.net,

French Data Network

v

Premier ministre,

Ministre de la Culture,

THE COURT (Full Court)

composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Arabadjiev, A. Prechal (Rapporteur), K. Jürimäe, C. Lycourgos, E. Regan, T. von Danwitz, F. Biltgen, N. Piçarra and Z. Csehi, Presidents of Chambers, M. Ilešič, J.-C. Bonichot, S. Rodin, P.G. Xuereb, L.S. Rossi, I. Jarukaitis, A. Kumin, N. Jääskinen, N. Wahl, I. Ziemele, J. Passer, D. Gratsias, M.L. Arastey Sahún and M. Gavalec, Judges,

Advocate General: M. Szpunar,

Registrars: V. Giacobbo and M. Krausenböck, Administrators,

having regard to the written procedure and further to the hearing on 5 July 2022,

after considering the observations submitted on behalf of:

– La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net and French Data Network, by A. Fitzjean Ó Cobhthaigh, avocat,

– the French Government, by A. Daniel, A.-L. Desjonquères and J. Illouz, acting as Agents,

– the Danish Government, by J.F. Kronborg and V. Pasternak Jørgensen, acting as Agents,

– the Estonian Government,, by M. Kriisa, acting as Agent,

– the Finnish Government, by H. Leppo, acting as Agent,

– the Swedish Government, by H. Shev, acting as Agent,

– the Norwegian Government, by F. Bergsjø, S.-E. Dahl, J.T. Kaasin and P. Wennerås, acting as Agents,

– the European Commission, by S.L. Kalėda, H. Kranenborg, P.-J. Loewenthal and F. Wilman, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 27 October 2022,

having regard to the order of 23 March 2023 to reopen the oral procedure, and further to the hearing on 15 May 2023,

after considering the observations submitted on behalf of:

– La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net and French Data Network, by A. Fitzjean Ó Cobhthaigh, avocat,

– the French Government, by R. Bénard, J. Illouz and T. Stéhelin, acting as Agents,

– the Czech Government, by T. Suchá and J. Vláčil, acting as Agents,

– the Danish Government, by J.F. Kronborg and C.A.-S. Maertens, acting as Agents,

– the Estonian Government, by M. Kriisa, acting as Agent,

– Ireland, by M. Browne, Chief State Solicitor, A. Joyce and D. O'Reilly, acting as Agents, and by D. Fenelly, Barrister-at-Law,

– the Spanish Government, by A. Gavela Llopis, acting as Agent,

– the Cypriot Government, by I. Neophytou, acting as Agent,

– the Latvian Government, by J. Davidoviča and K. Pommere, acting as Agents,

– the Netherlands Government, by E.M.M. Besselink, M.K. Bultermann and A. Hanje, acting as Agents,

– the Finnish Government, by A. Laine and H. Leppo, acting as Agents,

– the Swedish Government, by F.-D. Göransson and H. Shev, acting as Agents,

– the Norwegian Government, by S.-E. Dahl and P. Wennerås, acting as Agents,

– the European Commission, by S.L. Kalėda, H. Kranenborg, P.-J. Loewenthal and F. Wilman, acting as Agents,

– the European Data Protection Supervisor, by V. Bernardo, C.-A. Marnier, D. Nardi and M. Pollmann, acting as Agents,

– European Union Agency for Cybersecurity (ENISA), by A. Bourka, acting as Agent,

after hearing the Opinion of the Advocate General at the sitting on 28 September 2023,

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) ('Directive 2002/58'), read in the light of the Charter of Fundamental Rights of the European Union ('the Charter').

2 The request has been made in proceedings between the associations La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net and French Data Network, on the one hand, and the Premier ministre (Prime Minister, France) and the ministre de la Culture (Minister for Culture, France), on the other hand, concerning the legality of décret n° 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet » (Decree No 2010-236 of 5 March 2010 on the automated personal data processing system authorised by Article L. 331-29 of the code de la propriété intellectuelle (Intellectual Property Code), known as the 'System for the management of measures for the protection of works on the internet' (JORF No 56 of 7 March 2010, text No 19), as amended by décret n° 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 (Decree No 2017-924 of 6 May 2017 on the management of copyright and related rights by a rights management organisation and amending the Intellectual Property Code) (JORF No 109 of 10 May 2017, text No 176) ('Decree No 2010-236').

Legal context

European Union law

General rules concerning the protection of personal data

– *Directive 95/46/EC*

3 Article 7 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), contained in Section II of that directive, entitled 'Criteria for making data processing legitimate', was worded as follows:

'Member States shall provide that personal data may be processed only if:

…

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).'

4 Article 13(1) of that directive provides:

'Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary [measure] to safeguard:

…

(g) the protection of the data subject or the rights and freedoms of others.'

– *The GDPR*

5 Article 2 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; 'the GDPR'), entitled 'Material scope', provides, in paragraphs 1 and 2 thereof:

'1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

…

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

6 Article 4 of the GDPR, entitled 'Definitions', provides:

'For the purposes of this Regulation:

(1) “personal data” means any information relating to an identified or identifiable natural person (“data subject”); …

(2) “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

…’

7 Article 6 of that regulation, headed ‘Lawfulness of processing’, provides in paragraph 1:

‘Processing shall be lawful only if and to the extent that at least one of the following applies:

…

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data …

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.’

8 Article 9 of that regulation, entitled ‘Processing of special categories of personal data’, provides, in paragraph 2(e) and (f) thereof, that the prohibition on the processing of certain types of personal data revealing, inter alia, data concerning a natural person’s sexual life or sexual orientation does not apply where the processing relates to personal data which are manifestly made public by the data subject or is necessary, inter alia, for the establishment, exercise or defence of legal claims.

9 Article 23 of the GDPR, entitled ‘Restrictions’, provides, in paragraph 1 thereof:

‘Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

…

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.’

Sector-specific rules concerning the protection of personal data

– *Directive 2002/58*

10 Recitals 2, 6, 7, 11, 26 and 30 of Directive 2002/58 state:

‘(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by [the Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

…

(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

…

(11) Like Directive [95/46], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms [signed in Rome on 4 November 1950], as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

…

(26) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data … may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. …

…

(30) Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. …'

11 Article 2 of Directive 2002/58, headed 'Definitions', provides:

'…

The following definitions shall also apply:

(a) "user" means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

(b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) "location data" means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

…'

12 Article 3 of that directive, entitled 'Services concerned', provides:

‘This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.’

13 Article 5 of the directive, headed ‘Confidentiality of the communications’, provides:

‘1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

…

(3) Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. …’

14 Article 6 of Directive 2002/58, entitled ‘Traffic data’, provides:

‘1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

…

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.’

15 Article 15 of Directive 2002/58, headed ‘Application of certain provisions of Directive [95/46]’, provides:

‘1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period

justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) [TEU].

…

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive [95/46] shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

…’

– *Directive (EU) 2016/680*

16 Article 1 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89), entitled ‘Subject matter and objectives’, provides, in paragraph 1 thereof:

‘This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’

17 Article 3 of that directive, entitled ‘Definitions’, provides:

‘For the purposes of this Directive:

…

(7) “competent authority” means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

…’

Rules concerning the protection of intellectual property

18 Article 8 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigendum in OJ 2004 L 195, p. 16), headed ‘Right of information’, provides:

‘1. Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer …:

2. The information referred to in paragraph 1 shall, as appropriate, comprise:

(a) the names and addresses of the producers, manufacturers, distributors, suppliers and other previous holders of the goods or services, as well as the intended wholesalers and retailers;

…

3. Paragraphs 1 and 2 shall apply without prejudice to other statutory provisions which:

(a) grant the rightholder rights to receive fuller information;

(b) govern the use in civil or criminal proceedings of the information communicated pursuant to this Article;

(c) govern responsibility for misuse of the right of information; or

(d) afford an opportunity for refusing to provide information which would force the person referred to in paragraph 1 to admit to his/her own participation or that of his/her close relatives in an infringement of an intellectual property right; or

(e) govern the protection of confidentiality of information sources or the processing of personal data.'

French law

The CPI

19 Article L. 331-12 of the Intellectual Property Code, in the version in force on the date of the decision contested by the applicants in the main proceedings ('the CPI'), provides:

'The Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet [(High Authority for the dissemination of works and the protection of rights on the internet; "Hadopi")] is an independent public authority. …'

20 Article L. 331-13 of that code provides:

'[Hadopi] shall:

1. Encourage the development of legal offers and monitor the lawful and unlawful use of works and subject matter covered by a copyright or a related right on electronic communications networks used for the provision of online public communication services;

2. Protect such works and subject matter from infringements of those rights committed in electronic communications networks used for the provision of online public communications services;

…'

21 Under Article L. 331-15 of that code:

'[Hadopi] shall consist of a College and a Committee for the protection of rights. …

…

In the exercise of their functions, the members of the College and of the Committee for the protection of rights shall not receive instructions from any authority.'

22 The first paragraph of Article L. 331-17 of that code provides:

'The Committee for the protection of rights shall be responsible for taking the measures provided for in Article L. 331-25.'

23 Under Article L. 331-21 of the CPI:

'In order for the Committee for the protection of rights to carry out its duties, [Hadopi] shall be staffed by sworn public officials authorised by [its] President in accordance with conditions laid down by

decree made after hearing the Conseil d'État [(Council of State, France)]. …

The members of the Committee for the protection of rights and the officials mentioned in the previous paragraph shall receive referrals to the committee in the manner prescribed in Article L. 331-24. They shall examine the facts.

They may, where necessary for the purposes of the procedure, obtain any document, irrespective of the medium on which it is stored, including data that have been retained and processed by electronic communications operators pursuant to Article L. 34-1 of the code des postes et des communications électroniques [(Post and Electronic Communications Code)] and by the service providers mentioned in Article 6(I)(1) and (2) of Loi no 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [(Law No 2004-575 of 21 June 2004 promoting confidence in the digital economy)].

They may also obtain copies of the documents mentioned in the preceding paragraph.

They may, in particular, obtain from electronic communications operators the identity, postal address, email address and telephone number of the subscriber whose access to online public communications services has been used for the purposes of the reproduction, representation, making available or communication to the public of protected works or subject matter without the authorisation of the holders of the rights … where such authorisation is required.'

24 Article L. 331-24 of that code provides:

'The Committee for the protection of rights shall act upon referral by sworn and authorised agents … appointed by:

– lawfully constituted professional defence bodies;

– collective management organisations;

– the Centre national du cinéma et de l'image animée [(National Centre for Cinema and the Moving Image, France)].

The Committee for the protection of rights may also act on the basis of information forwarded to it by the procureur de la République [(Office of the Public Prosecutor, France)].

Offending conduct dating back more than six months may not be referred to it.'

25 Under Article L. 331-25 of that code, which governs the 'graduated response' procedure:

'Where the offending conduct referred to it is liable to constitute a failure to fulfil the obligation laid down in Article L. 336-3 [of the CPI], the Committee for the protection of rights may send the subscriber … a recommendation drawing his or her attention to the provisions of Article L. 336-3, ordering him or her to fulfil the obligation laid down in those provisions and warning him or her of the penalties which may be imposed pursuant to Articles L. 335-7 and L. 335-7-1. That recommendation shall also furnish information to the subscriber about lawfully available online cultural content, the existence of security measures to prevent failures to fulfil the obligation laid down in Article L. 336-3, and the risks to growth in artistic output and to the economy of the culture industry posed by practices that do not respect copyright and related rights.

If the subscriber again engages in conduct liable to constitute a failure to fulfil the obligation laid down in Article L. 336-3 within six months of the recommendation referred to in the first paragraph being sent, the Committee may issue a further recommendation by electronic means containing the same information as the previous recommendation … It must attach to that recommendation a letter delivered with signed confirmation of receipt or any other means capable of proving the date of service of that recommendation.

Recommendations issued on the basis of this article shall state the date and time when the conduct liable to constitute a failure to fulfil the obligation laid down in Article L. 336-3 were detected.

However, they shall not disclose the content of the protected works or subject matter affected by that failure. They shall state the telephone number, postal address and email address to which the recipient of the recommendation may direct, if he or she so wishes, his or her observations to the Committee for the protection of rights and obtain, upon express request, details of the content of the protected works or subject matter affected by the failure complained of.'

26 Article L. 331-29 of the CPI states:

'[Hadopi] is authorised to establish a system for the automated processing of personal data relating to individuals who are the subject of a procedure under this subsection.

The purpose of that processing shall be to enable the Committee for the protection of rights to implement the measures provided for in this subsection, to carry out any related procedural acts, and to implement the procedures for informing professional defence bodies and collective management organisations of any referrals to a judicial authority and of the notifications referred to in the fifth paragraph of Article L. 335-7.

Detailed rules for the application of this article shall be laid down by decree … Those rules shall state, inter alia:

– the categories of data that may be recorded and the period of time for which they may be retained;

– the parties to which those data may be communicated, which shall include providers of access to online public communications services;

– the manner in which the individuals concerned may exercise, before [Hadopi], their right of access to data concerning them …'

27 The first and second paragraphs of Article L. 335-2 of that code stipulate:

'Any edition of writings, musical compositions, drawings, paintings or any other production, printed or engraved in whole or in part, contrary to the laws and regulations relating to the authors' ownership, is a counterfeit and any counterfeiting is an offence.

The counterfeiting in France of works published in France or abroad is punishable by three years' imprisonment and a fine of EUR 300 000.'

28 The first paragraph of Article L. 335-4 of that code provides:

'Any fixation, reproduction, communication or making available to the public, whether for consideration or free of charge, or any television broadcast of a performance, phonogram, videogram, programme or press publication, made without the authorisation, where required, of the performer, the phonogram or videogram producer, the audiovisual communications undertaking, the press publisher or the news agency is punishable by three years' imprisonment and a fine of EUR 300 000.'

29 Article L. 335-7 of the CPI lays down the rules relating to the imposition, on persons guilty of the criminal offences referred to, inter alia, in Articles L. 335-2 and L. 335-4 of that code, of the additional penalty of suspension of access to an online public communication service for a maximum period of one year.

30 The first paragraph of Article L. 335-7-1 of that code reads as follows:

'In the case of minor offences in the fifth class provided for in this Code, where provided for by the regulations, the additional penalty defined in Article L. 335-7 may be imposed in accordance with the same rules, in the event of gross negligence, on the holder of access to an online public communication service to which the Committee for the protection of rights, pursuant to Article L. 331-25, has previously sent, by means of letter delivered with signed confirmation of receipt or any other means of

proving the date of submission, a recommendation asking him or her to implement a means of securing his or her internet access.'

31 Pursuant to Article L. 336-3 of that code:

'A person having a right of access to online public communications services is under an obligation to ensure that that access is not used for the purposes of the reproduction, representation, making available or communication to the public of works or subject matter protected by copyright or by a related right without the authorisation of the holders … where such authorisation is required.

Failure by the person having access to comply with the obligation set out in the first paragraph shall not have the effect of rendering him or her liable under criminal law …'

32 The first paragraph of Article R. 331-37 of the CPI provides:

'Electronic communications operators … and service providers … shall send, using a connection to the automated personal data processing system mentioned in Article L. 331-29 or using a recording medium which ensures their integrity and security, the personal data and the information mentioned in point 2 of the Annex to Decree [No 2010-236] within a period of eight days of receiving from the Committee for the protection of rights the technical data required to identify the subscriber whose access to online public communications services has been used for the purposes of the reproduction, representation, making available or communication to the public of protected works or subject matter without the authorisation of the holders of the rights … where such authorisation is required.'

33 Under Article R. 331-40 of that code:

'Where, within a period of one year following submission of the recommendation referred to in the first paragraph of Article L. 335-7-1, new offending conduct liable to constitute gross negligence as defined in Article R. 335-5 is referred to the Committee for the protection of rights, it shall inform the subscriber, by letter delivered with signed confirmation of receipt, that he or she may be prosecuted for that conduct. That letter shall invite the person concerned to submit his or her observations within 15 days. It shall state that he or she may, within the same period, request a hearing pursuant to Article L. 331-21-1 and that he or she is entitled to legal representation. It shall also invite the person concerned to specify his or her family responsibilities and resources.

The Committee for the protection of rights may, on its own initiative, invite the person concerned to attend a hearing. The letter of invitation shall state that the person concerned is entitled to be assisted by a lawyer.'

34 Article R. 335-5 of the CPI states:

'I. – Where the conditions laid down in paragraph II are met, gross negligence, punishable by the fine laid down for minor offences in the fifth class, shall be committed by a person having a right of access to online public communications services who, without legitimate reason:

1. has failed to establish measures to make such access secure; or

2. has failed to exercise due care in the implementation of those measures.

II. – The provisions of paragraph I shall not apply unless the following two conditions are met:

1. Under Article L. 331-25 and in accordance with the formal requirements laid down in that article, the Committee for the protection of rights has recommended to the person having a right of access to implement measures to make his or her access secure so as to prevent such access being used again for the purposes of the reproduction, representation, making available or communication to the public of works or subject matter protected by copyright or by a related right without the authorisation of the holders of those rights … where such authorisation is required;

2. During the year following receipt of that recommendation, that access is used on a further occasion for the purposes referred to in point 1 of paragraph II.'

35 With effect from 1 January 2022, pursuant to loi n° 2021-1382, du 25 octobre 2021, relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique [(Law No 2021-1382 of 25 October 2021 on the regulation and protection of access to cultural works in the digital era)] (JORF No 250 of 26 October 2021, text No 2), Hadopi was merged with the Conseil supérieur de l'audiovisuel (CSA) [(Higher Council for the audiovisual sector (CSA), France)], another independent public authority, to form the Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) [(Authority for the Regulation of Audiovisual and Digital Communications (ARCOM), France)].

36 The graduated response procedure, referred to in paragraph 25 above, has, however, remained essentially unchanged even though it is no longer implemented by Hadopi's Committee for the protection of rights, which was composed of three members appointed by the Conseil d'État (Council of State), the Cour des comptes (Court of Auditors, France) and the Cour de cassation (Court of Cassation, France) respectively, but rather by two members of the board of ARCOM, one of whom is appointed by the Conseil d'État (Council of State) and the other by the Cour de cassation (Court of Cassation).

Decree No 2010-236

37 Article 1 of Decree No 2010-236, adopted on the basis, inter alia, of Article L. 331-29 of the CPI, provides:

'The purpose of the personal data processing system known as the "System for the management of measures for the protection of works on the internet" is to enable the Commission for the protection of rights of [Hadopi]:

1. to implement the measures provided for in Book III of the legislative part of the [CPI] (Title III, Chapter I, Section 3, Subsection 3) and Book III of the regulatory part of that code (Title III, Chapter I, Section 2, Subsection 2);

2. to refer conduct liable to constitute an offence under Articles L. 335-2, L. 335-3, L. 335-4 and R. 335-5 of the [CPI] to the Office of the Public Prosecutor and to inform professional defence bodies and collective management organisations of those referrals;

…'

38 Article 4 of that decree provides:

'I. – The sworn public officials authorised by the President of [Hadopi] pursuant to Article L. 331-21 of the [CPI] and the members of the Committee for the protection of rights mentioned in Article 1 shall have direct access to the personal data and information referred to in the Annex to this Decree.

II – The electronic communications operators and the providers referred to in point 2 of the Annex to this Decree shall be sent:

– the technical data required to identify the subscriber;

– the recommendations provided for in Article L. 331-25 of the [CPI] for notification by electronic means to their subscribers;

– the information necessary for the implementation of additional penalties of suspension of access to an online public communications service notified to the Commission for the protection of rights by the Office of the Public Prosecutor.

III – Professional defence bodies and collective management organisations shall be informed of referrals to the Office of the Public Prosecutor.

IV – Judicial authorities shall be sent the reports of conduct liable to constitute an offence under Articles L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 and R. 335-5 of the [CPI].

The enforcement of a penalty of suspension shall be notified to the automated criminal records system.'

39 The annex to that decree provides:

'The personal data and information recorded in the processing system known as the "System for the management of measures for the protection of works on the internet" shall be as follows:

1. Personal data and information from lawfully constituted professional defence bodies, collective management organisations, the National Centre for Cinema and the Moving Image, and the Office of the Public Prosecutor:

Regarding conduct liable to constitute a failure to fulfil the obligation laid down in Article L. 336-3 of the [CPI]:

Date and time of the occurrence;

IP address of the subscribers concerned;

Peer-to-peer protocol used;

Pseudonym used by the subscriber;

Information on the protected works or subject matter affected by the conduct;

File name as it appears on the subscriber's device (where applicable);

Internet service provider through which access was arranged or which supplied the IP technical resource.

…

2. Personal data and information concerning the subscriber collected from electronic communications operators … and providers …:

Surname, forenames;

Postal address and email addresses;

Telephone number;

Address of the subscriber's telephone installation;

Internet service provider, using the technical facilities of the service provider referred to in point 1 with which the subscriber has taken out a contract; reference number;

start date of suspension of access to an online public communications service.

…'

The Post and Electronic Communications Code

40 Article L. 34-1, II *bis*, of the Post and Electronic Communications Code provides:

'Electronic communications operators shall retain:

1. for the purposes of criminal proceedings, preventing threats to public security and safeguarding national security, information relating to the user's civil identity until the expiry of a period of five years from the date on which his or her contract ends;

2. for the same purposes as those set out in paragraph II *bis*(1), other information supplied by the user when taking out a contract or creating an account and payment information until the expiry of a period of one year from the date on which his or her contract ends or his or her account is closed;

3. for the purposes of combating serious crime, preventing serious threats to public security and safeguarding national security, the technical data enabling the connection source to be identified or relating to the terminal equipment used until the expiry of a period of one year from the connection or use of the terminal equipment.'

The dispute in the main proceedings and the questions referred for a preliminary ruling

41 The Premier ministre (Prime Minister, France) having implicitly rejected their application for the repeal of Decree No 2010-236, the applicants in the main proceedings brought an action before the Conseil d'État (Council of State), by application of 12 August 2019, seeking the annulment of that implicit rejection decision. They claimed, in essence, that the third to fifth paragraphs of Article L. 331-21 of the CPI, which forms part of the legal basis of that decree, (i) is contrary to the right to respect for private life enshrined in the French Constitution and (ii) infringes EU law, in particular Article 15 of Directive 2002/58 and Articles 7, 8, 11 and 52 of the Charter.

42 As regards the part of the action relating to the alleged breach of the Constitution, the Conseil d'État (Council of State) referred a priority question on constitutionality to the Conseil constitutionnel (Constitutional Council, France).

43 By Decision No 2020-841 QPC of 20 May 2020, La Quadrature du Net et autres [Droit de communication à la Hadopi], the Conseil constitutionnel (Constitutional Council) declared the third and fourth paragraphs of Article L. 331-21 of the CPI contrary to the Constitution but declared the fifth paragraph of that article – with the exception of the words 'in particular' – consistent with the Constitution.

44 As regards the part of the action relating to the alleged infringement of EU law, the applicants in the main proceedings submitted, in particular, that Decree No 2010-236 and the provisions which constitute its legal basis permit access to connection data in a disproportionate manner for non-serious copyright offences committed on the internet, without prior review by a judge or an authority offering guarantees of independence and impartiality. In particular, those offences do not fall within the scope of 'serious crime' as referred to in the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970).

45 In that regard, the referring court, the Conseil d'État (Council of State), notes, first, that, in the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), the Court held, inter alia, that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude legislative measures which, for the purposes of safeguarding national security, combating crime and safeguarding public security, provide for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems. Accordingly, in the case of data relating to the civil identity of users of electronic communications systems, such retention is permissible, without any specific time limit being imposed, for the purposes of investigating, detecting and prosecuting criminal offences in general. Nor does Directive 2002/58 preclude access to those data for such purposes.

46 The referring court infers from this that, as regards access to data relating to the civil identity of users of electronic communications systems, the plea raised by the applicants in the main proceedings alleging that Decree No 2010-236 is unlawful since it was adopted in the context of action to combat non-serious offences must be rejected.

47 The referring court observes, secondly, that in the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), the Court held, inter alia, that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection and security of

traffic and location data and, in particular, access by the competent national authorities to retained data, where that access is not subject to a prior review by a court or an independent administrative body.

48 The referring court refers, more specifically, to paragraph 120 of that judgment, in which the Court stated that it is essential that such access to retained data should, as a general rule, except in cases of duly justified urgency, be subject to the requirement of a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime.

49 The Court referred to that requirement in the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), as regards the real-time collection of connection data by the intelligence services, and in the judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152), as regards access by national authorities to connection data.

50 The referring court also notes that Hadopi, since its establishment in 2009, has issued over 12.7 million recommendations to subscribers under the graduated response procedure provided for in Article L. 331-25 of the CPI, including 827 791 in 2019 alone. It follows that the officials of the Committee for the protection of rights of Hadopi have necessarily had to collect, each year, a considerable volume of data relating to the civil identity of the users concerned. The referring court considers that, in view of the volume of those recommendations, making such data collection subject to a prior review might make it impossible for recommendations to be issued at all.

51 In those circumstances, the Conseil d'État (Council of State) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

‘(1) Are the civil identity data corresponding to an IP address included among the traffic and location data to which, in principle, the requirement [of] prior review by a court or an independent administrative entity [whose decisions are binding] applies?

(2) If the first question is answered in the affirmative, and having regard to the fact that the data relating to the civil identity of users, including their contact details, are not particularly sensitive data, is Directive [2002/58], read in the light of the [Charter], to be interpreted as precluding national legislation which provides for the collection of those data, corresponding to the IP addresses of users, by an administrative authority, without prior review by a court or an independent administrative entity [whose decisions are binding]?

(3) If the second question is answered in the affirmative, and having regard to the fact that the data relating to civil identity are not particularly sensitive data, that only those data may be collected and they may be collected solely for the purposes of preventing failures to fulfil obligations which have been defined precisely, exhaustively and restrictively by national law, and that the systematic review of access to the data of each user by a court or a third-party administrative entity [whose decisions are binding] would be liable to jeopardise the fulfilment of the public service [mission] entrusted to the administrative authority which collects those data, which is itself independent, does [Directive 2002/58] preclude the review from being performed in an adapted fashion, for example as an automated review, as the case may be under the supervision of a department within the body which offers guarantees of independence and impartiality in relation to the officials who have the task of collecting the data?’

Consideration of the questions referred

52 By its three questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which authorises the public authority responsible for the protection of copyright and related rights against infringements of those rights committed on the internet to access data, retained by providers of publicly available electronic communications services, relating to the civil identity associated with IP addresses previously collected

by rightholder organisations, so that that public authority can identify the holders of those addresses – which have been used for activities liable to constitute such infringements – and may, where appropriate, take measures against them, without that access being subject to the requirement of a prior review by a court or an independent administrative body.

Preliminary observations

53 The case in the main proceedings involves two separate and successive personal data processing operations carried out in the context of the activities of Hadopi, an independent public authority whose mission, in accordance with Article L. 331-13 of the CPI, is to protect works and subject matter covered by copyright or related rights against infringements of those rights committed on electronic communications networks used for the provision of online public communication services.

54 The first processing operation, carried out upstream by sworn and authorised agents of rightholder organisations, takes place in two stages. First, IP addresses that appear to have been used for activities liable to constitute an infringement of copyright or related rights are collected on peer-to-peer networks. Secondly, a set of personal data and information are made available to Hadopi, in the form of reports. Those data are, according to the list in point 1 of the annex to Decree No 2010-236, the date and time of the occurrence, the IP address of the subscribers concerned, the peer-to-peer protocol used, the pseudonym used by the subscriber, information relating to the protected works or subject matter affected by the conduct, the file name as it appears on the subscriber's device (if applicable), and the internet service provider though which access was arranged or which supplied the IP technical resource.

55 The second processing operation, carried out downstream by the internet service providers at Hadopi's request, also takes place in two stages. First, the IP addresses collected upstream are matched with the holders of those addresses. Secondly, a set of personal data and information relating to those holders, concerning essentially their civil identity, is made available to that public authority. Those data are, according to the list set out in point 2 of the annex to Decree No 2010-236, essentially, the subscriber's surname and first names, postal address and email addresses, telephone number and the address of the subscriber's telephone installation.

56 Regarding the latter, the fifth paragraph of Article L. 331-21 of the CPI, in the version resulting from the decision of the Conseil constitutionnel (Constitutional Council) referred to in paragraph 43 above, provides that the members of Hadopi's Committee for the protection of rights and the sworn public officials of that authority authorised by its president may obtain from electronic communications operators the identity, postal address, email address and telephone number of the subscriber whose access to online public communication services has been used for the purposes of reproduction, representation, making available or communication to the public of protected works or subject matter without the authorisation of the rightholders where such authorisation is required.

57 Those different personal data processing operations are intended to enable Hadopi to take, with regard to the IP address holders thus identified, the measures provided for in the administrative procedure known as the 'graduated response' governed by Article L. 331-25 of the CPI. Those measures are, first of all, the sending of 'recommendations', which are similar to warnings; then, in the event of a referral to Hadopi's rights committee, within a period of one year following the sending of a second recommendation, in respect of conduct that may constitute a repetition of the offending conduct detected, the notification of the subscriber, as referred to in Article R. 331-40 of the CPI, that the conduct is liable to constitute the offence of 'gross negligence', defined in Article R. 335-5 of the CPI, a minor offence punishable by a maximum fine of EUR 1 500 and EUR 3 000 in the event of a repeat offence; and lastly, after deliberation, the referral to the public prosecution service of conduct that may constitute such a minor offence or, as the case may be, the offence of counterfeiting referred to in Article L. 335-2 of the CPI or Article L. 335-4 of that code, punishable by three years' imprisonment and a fine of EUR 300 000.

58 That being said, the questions raised by the referring court concern only the downstream processing described in paragraph 55 above and not the upstream processing, the essential characteristics of which were set out in paragraph 54 above.

59 It must however be noted that, if the prior collection of IP addresses by the rightholder organisations concerned were contrary to EU law, EU law would also preclude the use of those data in the context of the subsequent processing by providers of electronic communications services consisting in matching those addresses to data relating to the civil identity of the holders of those addresses.

60 In that context, it should be recalled at the outset that, according to the Court's case-law, IP addresses constitute both traffic data for the purposes of Directive 2002/58 and personal data for the purposes of the GDPR (see, to that effect, judgment of 17 June 2021, *M.I.C.M.*, C-597/19, EU:C:2021:492, paragraphs 102 and 113 and the case-law cited).

61 However, the collection of IP addresses which are public and visible to everyone, by agents of rightholder organisations, does not fall within the scope of Directive 2002/58, since such processing clearly does not take place 'in connection with the provision of … electronic communications services', within the meaning of Article 3 of that directive.

62 By contrast, such a collection of IP addresses, authorised, as can be seen from the documents before the Court, within certain quantitative limits and under certain conditions, by the Commission nationale de l'informatique et des libertés (CNIL) (National Commission for Information Technology and Civil Liberties (CNIL), France), with a view to their transmission to Hadopi for the purposes of their potential use in subsequent administrative or judicial proceedings intended to combat activities which infringe copyright and related rights, does constitute 'processing', within the meaning of Article 4(2) of the GDPR, the lawfulness of which depends on the conditions laid down in point (f) of the first subparagraph of Article 6(1) of that regulation, in the light of the Court's case-law set out, inter alia, in the judgments of 17 June 2021, *M.I.C.M.* (C-597/19, EU:C:2021:492, paragraphs 102 and 103), and of 4 July 2023, *Meta Platforms and Others (General terms of use of a social network) (*C-252/21, EU:C:2023:537, paragraphs 106 to 112 and the case-law cited).

63 As regards the downstream processing described in paragraph 55 above, it falls within the scope of Directive 2002/58 since it takes place 'in connection with the provision of … electronic communications services', within the meaning of Article 3 of that directive, inasmuch as the data at issue are obtained from providers of electronic communications services in accordance with Article L. 331-21 of the CPI.

Whether access by a public authority to data relating to the civil identity associated with an IP address retained by providers of electronic communications services for the purpose of combating counterfeiting offences committed online can be justified under Article 15(1) of Directive 2002/58

64 In the light of the foregoing preliminary observations, the question arises as to whether, as the referring court asks, the limitation on the fundamental rights enshrined in Articles 7, 8 and 11 of the Charter entailed by access by a public authority, such as Hadopi, to data relating to the civil identity associated with an IP address which it already has can be justified under Article 15(1) of Directive 2002/58.

65 Access to such personal data may be granted only in so far as they have been retained in a manner consistent with Directive 2002/58 (see, to that effect, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 29).

The requirements surrounding the retention of data relating to civil identity and associated IP addresses by providers of electronic communications services

66 Article 15(1) of Directive 2002/58 enables the Member States to introduce exceptions to the obligation of principle, laid down in Article 5(1) of that directive, to ensure the confidentiality of personal data, and to the corresponding obligations, referred to, inter alia, in Articles 6 and 9 of that directive, where such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. To that end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on one of those grounds. That being said, the option to derogate from the rights and obligations laid down in Articles 5, 6 and 9 of Directive 2002/58 cannot

permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and data relating thereto and, in particular, to the prohibition on storage of those data, explicitly laid down in Article 5 of that directive, to become the rule (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 110 and 111).

67 A legislative measure adopted under that provision must therefore correspond, genuinely and strictly, to one of the objectives mentioned in the preceding paragraph – the list of those objectives set out in the first sentence of Article 15(1) of Directive 2002/58 being exhaustive – and comply with the general principles of EU law, including the principle of proportionality, and the fundamental rights guaranteed by the Charter. In that regard, the Court has previously held that the obligation imposed on providers of electronic communications services by a Member State by way of national legislation to retain traffic data for the purpose of making them available, if necessary, to the competent national authorities raises issues relating to compatibility not only with Articles 7 and 8 of the Charter, relating to the protection of privacy and to the protection of personal data, respectively, but also with Article 11 of the Charter, relating to the freedom of expression (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 112 and 113).

68 Thus, the interpretation of Article 15(1) of Directive 2002/58 must take account of the importance both of the right to respect for private life, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 thereof, as derived from the case-law of the Court, as well as the importance of the right to freedom of expression, given that that fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 114 and the case-law cited).

69 It should be emphasised, in that regard, that the retention of traffic and location data constitutes, in itself, first, a derogation from the prohibition laid down in Article 5(1) of Directive 2002/58 barring any person other than the user from storing those data, and, secondly, an interference with the fundamental rights to respect for private life and protection of personal data, enshrined in Articles 7 and 8 of the Charter, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference. Whether or not the retained data have been used subsequently is also irrelevant, since access to such data is a separate interference with the fundamental rights referred to in the preceding paragraph, irrespective of the subsequent use made of those data (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 115 and 116).

70 That being said, in so far as Article 15(1) of Directive 2002/58 allows Member States to introduce certain derogating measures, as noted in paragraph 66 above, that provision reflects the fact that the rights enshrined in Articles 7, 8 and 11 of the Charter are not absolute rights, but must be considered in relation to their function in society. Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 120 and 121).

71 In the present case, it should be noted that although, formally, Hadopi is authorised to access only data relating to the civil identity associated with an IP address, that access has the particular feature that it first requires the providers of electronic communications services concerned to match the IP address with the civil identity data of the holder of that address. That access therefore necessarily presupposes that the providers have the IP addresses as well as the data relating to the identity of the holders of those addresses.

72 In addition, that public authority seeks access to those data for the sole purpose of identifying the holder of an IP address which has been used for activities liable to infringe copyright or related rights,

since he or she has unlawfully made protected works available on the internet for downloading by others. In those circumstances, the data relating to civil identity must be regarded as being closely linked both to the IP address and to the information that Hadopi has concerning the work made available on the internet.

73 That particular context cannot be ignored when examining the possible justification for a measure providing for the retention of personal data under Article 15(1) of Directive 2002/58, interpreted in the light of Articles 7, 8 and 11 of the Charter (see, by analogy, ECtHR, 24 April 2018, *Benedik v. Slovenia*, CE:ECHR:2018:0424JUD006235714, § 109).

74 Accordingly, it is in the light of the requirements arising, as regards the retention of IP addresses, from Article 15(1) of Directive 2002/58, interpreted in the light of Articles 7, 8 and 11 of the Charter, that it is necessary to examine any justification for the interference with the fundamental rights enshrined in those articles of the Charter entailed by the retention, by providers of publicly available electronic communications services, of data which Hadopi has the power to access.

75 In that context, it should be noted that, according to the Court's case-law, although, as noted in paragraph 60 above, IP addresses constitute traffic data for the purposes of Directive 2002/58, they are distinct from other categories of traffic data and location data.

76 In that regard, the Court has held that IP addresses are generated independently of any particular communication and mainly serve to identify, through providers of electronic communications services, the owner of the terminal equipment from which an internet communication is made. Thus, in relation to email and internet telephony, provided that only the IP addresses of the source of the communication are retained and not the IP addresses of the recipient of the communication, those addresses do not, as such, disclose any information about third parties who were in contact with the person who made the communication. To that extent, that category of data is less sensitive than other traffic data (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 152).

77 It is true that, in paragraph 156 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), the Court held that, despite the finding that IP addresses are less sensitive when they serve exclusively to identify the user of an electronic communications service, Article 15(1) of Directive 2002/58 precludes the general and indiscriminate retention of only IP addresses assigned to the source of a connection for purposes other than action to combat serious crime, the prevention of serious threats to public security or the safeguarding of national security. However, in reaching that conclusion, the Court expressly relied on the serious nature of the interference with the fundamental rights enshrined in Articles 7, 8 and 11 of the Charter which such retention of IP addresses is likely to entail.

78 The Court considered, in paragraph 153 of the same judgment, that, since IP addresses may, inter alia, when used to 'track an internet user's complete clickstream' and, therefore, his or her online activity, enable a 'detailed profile' of the user to be produced, the retention and analysis of those IP addresses which is required for such tracking constitute a serious interference with the fundamental rights of the internet user enshrined in Articles 7 and 8 of the Charter, which may also deter users of electronic communication systems from exercising their freedom of expression guaranteed by Article 11 of the Charter.

79 However, it must be noted that the general and indiscriminate retention of a set – even a vast set – of static and dynamic IP addresses used by a person in a given period does not necessarily constitute, in every case, a serious interference with the fundamental rights guaranteed by Articles 7, 8 and 11 of the Charter.

80 In that regard, first of all, the cases that gave rise to the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), concerned national legislation which involved an obligation to retain a set of data necessary to determine the date, time, duration and type of communication, to identify the communications equipment used and to determine the location of the terminal equipment and the communications, data which included, inter alia, the name and address of the user, the telephone numbers of the caller and the person called and the IP address for

internet services. Moreover, in two of those cases, the national legislation at issue also appeared to cover data relating to the conveyance of electronic communications by networks, which also enables the nature of the information consulted online to be identified (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 82 and 83).

81 The retention of IP addresses under such national legislation was therefore such – in view of the other data which those rules required to be retained and the possibility of combining those various data – as to allow precise conclusions to be drawn about the private life of the persons whose data were concerned and, consequently, to lead to a serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, concerning the protection of the privacy and personal data of those persons, and in Article 11 of that Charter, concerning their freedom of expression.

82 By contrast, an obligation imposed on providers of electronic communications services, by a legislative measure under Article 15(1) of Directive 2002/58, to ensure the general and indiscriminate retention of IP addresses may, as the case may be, be justified by the objective of combating criminal offences in general where it is genuinely ruled out that that retention could give rise to serious interferences with the private life of the person concerned due to the possibility of drawing precise conclusions about that person by, inter alia, linking those IP addresses with a set of traffic or location data which have also been retained by those providers.

83 Accordingly, a Member State which seeks to impose on providers of electronic communications services an obligation to retain IP addresses, in a general and indiscriminate manner, in order to achieve an objective linked to combating criminal offences in general must ensure that the arrangements for the retention of those data are such as to ensure that any combination of those IP addresses with other data, retained in compliance with Directive 2002/58, which would allow precise conclusions to be drawn about the private life of the persons whose data are thus retained, is ruled out.

84 In order to ensure that such a combination of data allowing precise conclusions to be drawn about the private life of the person concerned is ruled out, the retention arrangements must relate to the very manner in which the retention is structured; in essence, that retention must be organised in such a way as to guarantee a genuinely watertight separation of the different categories of data retained.

85 In that regard, it is indeed for the Member State which seeks to impose on providers of electronic communications services an obligation to retain IP addresses, in a general and indiscriminate manner, in order to attain an objective linked to combating criminal offences in general, to lay down, in its legislation, clear and precise rules relating to those retention arrangements, which must meet strict requirements. The Court may, however, provide clarifications regarding those arrangements.

86 In the first place, the national rules referred to in the preceding paragraph must ensure that each category of data, including data relating to civil identity and IP addresses, is kept completely separate from the other categories of data retained.

87 In the second place, those rules must ensure that, from a technical point of view, the separation of the various categories of retained data, in particular data relating to civil identity, IP addresses, the various traffic data other than IP addresses and the various location data, is genuinely watertight, by means of a secure and reliable computer system.

88 In the third place, in so far as those rules provide for the possibility of linking the retained IP addresses with the civil identity of the person concerned in compliance with the requirements stemming from Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 of the Charter, they must permit such linking only through the use of an effective technical process which does not undermine the effectiveness of the watertight separation of those categories of data.

89 In the fourth place, the reliability of that watertight separation must be subject to regular review by a public authority other than that which seeks to obtain access to the personal data retained by the providers of electronic communications services.

90 In so far as the applicable national legislation provides for such strict requirements relating to the arrangements for the general and indiscriminate retention of IP addresses and other data retained by providers of electronic communications services, the interference resulting from that retention of IP addresses cannot, due to the very manner in which that retention is structured, be categorised as 'serious'.

91 Where such a legislative framework is introduced, the arrangements for the retention of IP addresses thus prescribed rule out the possibility that those data might be combined with other data retained in compliance with Directive 2002/58, allowing precise conclusions to be drawn about the private life of the person concerned.

92 Consequently, in the presence of a legislative framework meeting the requirements set out in paragraphs 86 to 89 above, ensuring that no combination of data will allow precise conclusions to be drawn about the private life of the persons in question, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 of the Charter, does not preclude the Member State concerned from imposing an obligation to retain IP addresses, in a general and indiscriminate manner, for the purposes of combating criminal offences in general.

93 Lastly, such a legislative framework must, as is apparent from paragraph 168 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), provide for a retention period limited to what is strictly necessary and ensure, by means of clear and precise rules, that the retention of the data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse and against any unlawful access to or use of those data.

94 It is for the national court to ascertain whether the national legislation at issue in the main proceedings comply with the requirements referred to in paragraphs 85 to 93 above.

The requirements surrounding access to data relating to the civil identity associated with an IP address retained by providers of electronic communications services

95 It follows from the Court's case-law that, in the field of combating criminal offences, only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying the serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter entailed by public authorities having access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and that allow precise conclusions to be drawn concerning the private life of the persons concerned, and other factors relating to the proportionality of a request for access, such as the length of the period in respect of which access to such data is sought, cannot have the effect that the objective of preventing, investigating, detecting and prosecuting criminal offences in general is capable of justifying such access (judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 35).

96 However, where the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter entailed by a public authority's access to data relating to civil identity retained by providers of electronic communications services, without it being possible for those data to be associated with information on the communications made, is not serious since, taken as a whole, those data do not allow precise conclusions to be drawn concerning the private life of the persons whose data are concerned, that access may be justified by an objective of prevention, investigation, detection and prosecution of criminal offences in general (see, to that effect, judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraphs 54, 57 and 60).

97 It should also be added that, according to a principle established in the Court's settled case-law, access to traffic and location data may be justified under Article 15(1) of Directive 2002/58 only by the public interest objective for which the providers of electronic communications services were ordered to retain those data, except where that access is justified by a more important public interest objective. It follows, inter alia, from that principle that such access may in no event be granted for the purpose of combating offences in general where the retention of those data was justified by the objective of

combating serious crime or, a fortiori, by the objective of safeguarding national security (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 166).

98 However, that objective of combating criminal offences in general is capable of justifying the grant of access to traffic and location data which were stored and thus retained to the extent and for the time necessary for the marketing and billing of services and the provision of value added services, as authorised by Article 6 of Directive 2002/58 (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 108 and 167).

99 In the present case, in the first place, it is apparent from the national legislation at issue in the main proceedings that Hadopi does not have access to a 'set of traffic or location data', within the meaning of the case-law referred to in paragraph 95 above, with the result that it cannot, in principle, draw precise conclusions about the private life of the persons concerned. Access which does not allow such conclusions to be drawn does not constitute a serious interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter.

100 According to that legislation and the explanations provided by the French Government in that regard, the access granted to that public authority is strictly limited to certain data relating to the civil identity of the holder of an IP address and is authorised for the sole purpose of enabling the identification of that holder suspected of having engaged in an activity infringing copyright or related rights in that he or she has unlawfully made protected works available on the internet, for downloading by others. The purpose of that access is the adoption, where appropriate, of one of the educational or punitive measures provided for in the context of the graduated response procedure in respect of that holder, namely the sending of a first and second recommendation and then a letter notifying him or her that that activity is liable to constitute the minor offence of gross negligence and, lastly, the referral of the matter to the public prosecution service for the prosecution of that minor offence or the offence of counterfeiting.

101 That national legislation must also lay down clear and precise rules capable of ensuring that the IP addresses retained in accordance with Directive 2002/58 can be used only to identify the person to whom a particular IP address was assigned, while precluding any use that allows the surveillance, by means of one or more of those addresses, of that person's online activity. Where an IP address is thus used for the sole purpose of identifying its holder in the context of a specific administrative procedure which may give rise to criminal proceedings against the person concerned and not for purposes such as, for example, identifying the contacts or location of that holder, the access to that address for that sole purpose concerns that address as data relating to civil identity rather than as traffic data.

102 In addition, it follows from the principle established in the settled case-law referred to in paragraph 97 above that access such as that enjoyed by Hadopi under the national legislation at issue in the main proceedings, since it pursues the objective of combating criminal offences in general, can be justified only if it concerns IP addresses which must be retained by providers of electronic communications services for the purposes of that objective and not for the purposes of a more important objective such as that of combating serious crime, without prejudice however to access justified by such an objective of combating offences in general where it relates to IP addresses stored and therefore retained under the conditions laid down in Article 6 of Directive 2002/58.

103 Moreover, as can be seen from paragraphs 85 to 92 above, the retention of IP addresses, based on a legislative measure under Article 15(1) of Directive 2002/58, for the purposes of the objective of combating criminal offences in general, may be justified where the arrangements for that retention introduced by the legislative framework concerned meet a set of requirements intended to ensure, in essence, a genuinely watertight separation of the different categories of data retained, such that the combination of data belonging to different categories is genuinely ruled out. Where such retention arrangements are imposed on providers of electronic communications services, the general and indiscriminate retention of IP addresses does not constitute a serious interference with the privacy of the holders of those addresses, since those data do not allow precise conclusions to be drawn about their private life.

104 Accordingly, in the light of the case-law referred to in paragraphs 95 to 97 above, where such a legislative framework is established, access to the IP addresses retained for the purposes of the objective of combating criminal offences in general may be justified as regards Article 15(1) of Directive 2002/58 where that access is authorised for the sole purpose of identifying the person suspected of being involved in such offences.

105 Moreover, allowing a public authority such as Hadopi to have access to data relating to the civil identity associated with a public IP address sent to it by rightholder organisations for the sole purpose of identifying the holder of that address used for online activities liable to infringe copyright or related rights, with a view to imposing on him or her one of the measures provided for under the graduated response procedure, is consistent with the Court's case-law concerning the 'right of information' in the context of proceedings concerning an infringement of an intellectual property right as provided for in Article 8 of Directive 2004/48 (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 47 et seq.).

106 In that case-law, while emphasising that the application of the measures provided for by Directive 2004/48 cannot affect the GDPR or Directive 2002/58, the Court held that Article 8(3) of Directive 2004/48, read in conjunction with Article 15(1) of Directive 2002/58 and Article 7(f) of Directive 95/46, does not preclude Member States from imposing an obligation on providers of electronic communications services to disclose personal data to private persons in order to enable them to bring civil proceedings for copyright infringements, but nor does it require those Member States to lay down such an obligation (see, to that effect, judgment of 17 June 2021, *M.I.C.M.*, C-597/19, EU:C:2021:492, paragraphs 124 and 125 and the case-law cited).

107 That being said, in the second place, for the purposes of the specific assessment of the extent of the interference with privacy entailed by a public authority's access to personal data, the particular context in which that access takes place and, in particular, all the data and information communicated to that authority pursuant to the applicable national legislation, including pre-existing content-revealing data and information, cannot be ignored (see, by analogy, ECtHR, 24 April 2018, *Benedik v. Slovenia*, CE:ECHR:2018:0424JUD006235714, § 109).

108 Thus, in the present case, it is necessary to take into account, for the purposes of that assessment, the fact that, prior to accessing the data relating to the civil identity in question available to it, Hadopi receives from the rightholder organisations, inter alia, 'information on the protected works or subject matter affected by the conduct' and, 'where applicable', the 'file name as it appears on the subscriber's device', in accordance with point 1 of the annex to Decree No 2010-236.

109 It appears from the documents before the Court, subject to verification by the referring court, that the information on the work concerned – as recorded in a report whose content is governed by the deliberations of the CNIL of 10 June 2010 – is limited, essentially, to the title of the work concerned and an extract known as a 'chunk', in the form of an alphanumeric sequence and not an audio or video capture of the work.

110 In that regard, it is true that it cannot, broadly speaking, be ruled out that access by a public authority to a limited number of data relating to the civil identity of a holder of an IP address notified to that authority by a provider of electronic communications services for the sole purpose of identifying the holder of that address where it has been used for activities liable to infringe copyright or related rights, if it is combined with an analysis of even limited information on the content of the work unlawfully made available on the internet which was sent to that authority previously by the rightholder organisations, may reveal to that public authority certain aspects of the private life of that holder, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health. Moreover, such data enjoys special protection under EU law.

111 However, in the present case, in view of the nature of the limited data and information available to Hadopi, it is only in atypical situations that they are liable to reveal potentially sensitive information about aspects of the private life of the individual in question that, taken together, could enable that public authority to draw precise conclusions about his or her private life, for example by establishing a detailed profile of that person.

112 That could be the case, inter alia, with regard to a person whose IP address has been used for activities infringing copyright or related rights on peer-to-peer networks repeatedly, or on a large scale, in connection with protected works of particular types that can be grouped together on the basis of the words in their title that are liable to reveal potentially sensitive information about aspects of his or her private life.

113 That being said, various factors support the view that, in the present case, the interference with the privacy of a person suspected of having engaged in an activity infringing copyright or related rights permitted by legislation such as that at issue in the main proceedings is not necessarily of a high degree of seriousness. First of all, in accordance with that legislation, Hadopi's access to the personal data at issue is restricted to a limited number of authorised and sworn officials of that public authority, a body which moreover has independent status in accordance with Article L. 331-12 of the CPI. Next, the sole purpose of that access is to identify a person suspected of having engaged in an activity infringing copyright or related rights where it is found that a protected work has been unlawfully made available from that person's internet connection. Lastly, Hadopi's access to the personal data at issue is strictly limited to the data necessary for that purpose (see, by analogy, ECtHR, 17 October 2019, *López Ribalda and Others v. Spain*, CE:ECHR:2019:1017JUD000187413, §§ 126 and 127).

114 Another factor capable of further reducing the degree of interference with the fundamental rights to the protection of privacy and personal data resulting from that access by Hadopi – which appears to follow from the documents before the Court but which it is for the referring court to verify – concerns the fact that, under the applicable national legislation, Hadopi officials who have access to the data and information concerned are bound by an obligation of confidentiality prohibiting them from disclosing those data and information in any form whatsoever, except for the sole purpose of referring the matter to the public prosecution service, and from using them for purposes other than the identification of the IP address holder suspected of having engaged in an activity infringing copyright or a related right in order to impose on him or her one of the measures provided for in the context of the graduated response procedure (see, by analogy, ECtHR, 17 December 2009, *Gardel v. France*, CE:ECHR:2009:1217JUD001642805, § 70).

115 Thus, in so far as national legislation satisfies the conditions set out in paragraph 101 above, the IP addresses communicated to a public authority such as Hadopi do not make it possible to track the clickstream of the holder of those addresses, which tends to confirm the finding that the interference entailed by that authority's access to the identification data at issue in the main proceedings cannot be classified as serious.

116 In the third place, it must be borne in mind that, in order to strike the necessary balance between the rights and interests at issue imposed by the requirement of proportionality laid down in the first sentence of Article 15(1) of Directive 2002/58, even though the freedom of expression and the confidentiality of personal data are primary considerations and users of telecommunications and internet services must have a guarantee that their privacy and freedom of expression will be respected, those fundamental rights are nevertheless not absolute. In balancing the rights and interests at issue, those fundamental rights must yield on occasion to other fundamental rights or public-interest imperatives, such as the maintenance of public order and the prevention of crime or the protection of the rights and freedoms of others. This is, in particular, the case where the weight given to those primary considerations is such as to hinder the effectiveness of a criminal investigation, in particular by making it impossible or excessively difficult to identify effectively the perpetrator of a criminal offence and to impose a penalty on him or her (see, by analogy, ECtHR, 2 March 2009, *K.U. v. Finland*, CE:ECHR:2008:1202JUD000287202, § 49).

117 In that context, due account must be taken of the fact that, as the Court has already held, as regards offences committed online, accessing the IP addresses may be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be effectively identified (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 154).

118 That tends to show, as the Advocate General also pointed out, in essence, in point 59 of his Opinion of 28 September 2023, that the retention of and access to those IP addresses are – as regards combating

criminal offences such as offences infringing copyright or related rights committed online – strictly necessary for the attainment of the objective pursued and therefore meet the requirement of proportionality imposed by Article 15(1) of Directive 2002/58, read in the light of recital 11 of that directive and Article 52(2) of the Charter.

119 Moreover, as the Advocate General emphasised, in essence, in points 78 to 80 of his Opinion of 27 October 2022 and in points 80 and 81 of his Opinion of 28 September 2023, not to allow such access would carry a real risk of systemic impunity not only for criminal offences infringing copyright or related rights, but also for other types of criminal offences committed online or the commission or preparation of which is facilitated by the specific characteristics of the internet. The existence of such a risk constitutes a relevant factor for the purposes of assessing, when balancing the various rights and interests in question, whether an interference with the rights guaranteed by Articles 7, 8 and 11 of the Charter is a proportionate measure in the light of the objective of combating criminal offences.

120 It is true that access by a public authority such as Hadopi to civil identity data associated with the IP address from which the online offence was committed is not necessarily the only possible means of investigation in order to identify the person holding that address at the time that offence was committed. Such identification could also be possible, on the face of it, by examining all the online activities of the person concerned, in particular by analysing the ‘tracks’ which that person might have left on social media, such as the username used on those networks or his or her contact details.

121 However, as the Advocate General observed in point 83 of his Opinion of 28 September 2023, such a means of investigation would be particularly intrusive since it could reveal precise information on the private life of the persons concerned. It would thus entail, for those persons, a more serious interference with the rights guaranteed in Articles 7, 8 and 11 of the Charter than would follow from legislation such as that at issue in the main proceedings.

122 It follows from the foregoing that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter must be interpreted as meaning that it does not preclude, in principle, national legislation allowing a public authority responsible for the protection of copyright and related rights against infringements of those rights committed on the internet to access data relating to the civil identity associated with IP addresses previously collected by rightholder organisations and retained by the providers of electronic communications services in a separate and genuinely watertight manner, for the sole purpose of enabling that authority to identify the holders of those addresses suspected of being responsible for those infringements and, where appropriate, to take measures in that regard. In that case, the national legislation must prohibit the officials having such access (i) from disclosing in any form whatsoever information concerning the content of the files consulted by those holders except for the sole purpose of referring the matter to the public prosecution service, (ii) from tracking in any way the clickstream of those holders and (iii) from using those IP addresses for purposes other than the adoption of those measures.

The requirement of a prior review by a court or an independent administrative body before a public authority accesses data relating to the civil identity associated with an IP address

123 The question arises, however, whether access by the public authority to data relating to the civil identity associated with an IP address must also be subject to a prior review by a court or by an independent administrative body.

124 In that regard, it is in order to ensure, in practice, full observance of the conditions which the Member States are required to establish in order to ensure that the access is limited to what is strictly necessary that the Court has held that it is ‘essential’ that access by competent national authorities to traffic and location data be subject to a prior review carried out either by a court or by an independent administrative body (see, to that effect, judgments of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 120; of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 189; of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 51; and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 106).

125 That prior review requires, first, that the court or independent administrative body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various legitimate interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or that body must be able to strike a fair balance between, on the one hand, the legitimate interests relating to the needs of the investigation in the context of combating crime and, on the other hand, the fundamental rights to respect for private life and protection of personal data of the persons whose data are concerned by the access (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 107 and the case-law cited).

126 Secondly, where that review is carried out not by a court but by an independent administrative body, that body must have a status that enables it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence. Accordingly, it follows that the requirement of independence that has to be satisfied by the body entrusted with carrying out the prior review means that that body must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field the requirement of independence entails that the body entrusted with the prior review, first, should not be involved in the conduct of the criminal investigation in question and, secondly, must have a neutral stance vis-à-vis the parties to the criminal proceedings (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 108 and the case-law cited).

127 Thirdly, the independent review required in accordance with Article 15(1) of Directive 2002/58 must take place before any access to the data concerned, except in the event of duly justified urgency, in which case the review must take place within a short time. A subsequent review would not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 110).

128 That being said, although, as can be seen from the case-law referred to in paragraph 124 above, the Court has held that it is ‘essential’ that access by competent national authorities to traffic and location data be subject to a prior review carried out either by a court or by an independent administrative body, that case-law developed in the context of national measures allowing, for the purposes of an objective linked to combating serious crime, general access to all retained traffic and location data, regardless of whether there was any link with the objective pursued, and which thus entailed serious and even ‘particularly serious’ interferences with the fundamental rights concerned.

129 By contrast, in cases which concerned the conditions under which access to data relating to civil identity could be justified under Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 of the Charter, no express reference was made by the Court to the requirement of such a prior review (see, to that effect, judgments of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraphs 59, 60 and 62; of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 157 and 158; and of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 34).

130 It follows from the Court’s case-law relating to the principle of proportionality, compliance with which is required by the first sentence of Article 15(1) of Directive 2002/58 – in particular the case-law according to which the question whether the Member States may justify a limitation on the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of that directive must be assessed by measuring the seriousness of the interference with the fundamental rights laid down in Articles 7, 8 and 11 of the Charter entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to that seriousness (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 131) – that the degree of interference with the fundamental rights concerned entailed by access to the personal data in question and the degree of sensitivity of those data must also influence the substantive and procedural safeguards to which that access has to be subject, including the requirement of a prior review by a court or an independent administrative body.

131 Accordingly, having regard to that principle of proportionality, it must be held that the requirement of a prior review by a court or by an independent administrative body is necessary where, in the context of national legislation allowing a public authority to access personal data, that access carries the risk of a serious interference with the fundamental rights of the person concerned in that it could allow that public authority to draw precise conclusions about the private life of that person and, as the case may be, to establish a detailed profile of that person.

132 Conversely, that requirement of prior review is not intended to apply where the interference with the fundamental rights concerned entailed by access by a public authority to personal data cannot be classified as serious.

133 That is the case for access to data relating to the civil identity of users of electronic communications for the sole purpose of identifying the user concerned, and without it being possible for those data to be associated with information on the communications made, since, according to the case-law of the Court, the interference entailed by such processing of those data cannot, in principle, be classified as serious (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 157 and 158).

134 It follows that, where a retention framework as described in paragraphs 86 to 89 above is put in place, access by the public authority to the data relating to the civil identity associated with the IP addresses thus retained is not, in principle, subject to the requirement of prior review by a court or by an independent administrative body.

135 That being said, as noted in paragraphs 110 and 111 above, it cannot be ruled out that, in atypical situations, the limited data and information made available to a public authority in the context of a procedure such as the graduated response procedure at issue in the main proceedings may be liable to reveal potentially sensitive information concerning aspects of the private life of the person concerned which, taken together, could enable that public authority to draw precise conclusions about that person's private life and, as the case may be, to establish a detailed profile of that person.

136 As noted in paragraph 112 above, such a risk to privacy may arise, inter alia, where a person engages in activities infringing copyright or related rights on peer-to-peer networks repeatedly, or on a large scale, in connection with protected works of particular types that can be grouped together on the basis of the words in their title, revealing potentially sensitive information about aspects of that person's private life.

137 Thus, in the present case, in the context of the graduated response administrative procedure, a holder of an IP address may be particularly exposed to such a risk to his or her privacy where that procedure reaches the stage at which Hadopi must decide whether or not to refer the matter to the public prosecution service with a view to the prosecution of that person for conduct liable to constitute the minor offence of gross negligence or the offence of counterfeiting.

138 That referral presupposes that the holder of an IP address has already received two recommendations and a notification letter informing that person that his or her activities are liable to criminal prosecution, measures which imply that, on each occasion, Hadopi has had access to data relating to the civil identity of that person whose IP address has been used for activities infringing copyright or related rights and to a file relating to the work in question containing, essentially, its title.

139 It cannot be ruled out that, taken together and as the graduated response administrative procedure unfolds, the data thus provided in the various phases of that procedure may reveal concordant and potentially sensitive information about aspects of the private life of the person concerned thus making it possible to establish a profile of that person.

140 Thus, the intensity of the infringement of the right to respect for private life is likely to increase as the graduated response procedure, which is a sequential process, progresses through its various stages.

141 In the present case, Hadopi's access to all of the data relating to the person concerned collected during the various stages of that procedure may, by the linking of those data, be liable to enable precise conclusions to be drawn about the private life of that person. Accordingly, in the context of a procedure

such as the graduated response procedure at issue in the main proceedings, the national legislation must also provide for a prior review by a court or an independent administrative body, meeting the conditions set out in paragraphs 125 to 127 above, at a certain stage of that procedure, in order to rule out the risks of disproportionate interferences with the fundamental rights to the protection of privacy and personal data of the person concerned. That means that, in practice, such a review must take place before Hadopi can link the civil identity data of a person associated with an IP address and obtained from a provider of electronic communications services – that person having already been the subject of two recommendations – and the file relating to the work made available on the internet for downloading by others. Accordingly, that review must take place before sending a notification letter as referred to in Article R. 331-40 of the CPI, declaring that that person has engaged in conduct liable to constitute the minor offence of gross negligence. It is only following such a prior review by a court or an independent administrative authority and the authorisation of that court or administrative authority that Hadopi will be able to send such a letter and then, if necessary, refer the matter to the public prosecution service with a view to the prosecution of that offence.

142 Hadopi should be permitted to identify the cases in which the holder of the IP address concerned reaches that third stage of such a graduated response procedure. Accordingly, that procedure must be organised and structured in such a way that the civil identity data of a person associated with IP addresses previously collected on the internet, obtained from providers of electronic communications services, cannot automatically be linked, by the persons responsible for the examination of the facts within Hadopi, with the files containing information that reveals the titles of the protected works the making available of which on the internet justified that collection of IP addresses.

143 Thus, that linking for the purposes of the third stage of the graduated procedure must be suspended when the obtention of those civil identity data, corresponding to a case in which an activity infringing copyright or related rights has possibly been repeated for a second time, triggers the requirement of a prior review by a court or an independent administrative body described in paragraph 141 above.

144 In addition, the organisation of the requirement for prior review referred to in paragraphs 141 to 143 above, since it is limited to the third stage of the graduated response procedure and does not apply to the previous stages of that procedure, also allows account to be taken of the argument that it is necessary to ensure the practicability of that procedure, which is characterised – especially in the stages prior to the potential dispatch of the notification letter and, as the case may be, the referral of the matter to the public prosecution service – by the massive number of requests for access from the public authority resulting from the equally large number of reports referred to it by the rightholder organisations.

145 Furthermore, as regards the object of the prior review referred to in paragraphs 141 to 143 above, it follows from the case-law referred to in paragraphs 95 and 96 above that, where the person concerned is suspected of having committed the offence of ‘gross negligence’ defined in Article R. 335-5 of the CPI, which falls within the scope of criminal offences in general, the court or independent administrative body responsible for that review must refuse access where that access would allow the public authority which sought it to draw precise conclusions about the private life of that person.

146 However, even access allowing such precise conclusions to be drawn should be authorised in cases where the evidence before that court or independent administrative body supports the suspicion that the person has committed the offence of counterfeiting referred to in Article L. 335-2 of the CPI or Article L. 335-4 of that code, given that it is permissible for a Member State to consider that such an offence, inasmuch as it undermines a fundamental interest of society, constitutes a serious crime.

147 Lastly, as regards the manner in which that prior review is to be carried out, the French Government submits that, in view of the particular characteristics of Hadopi’s access to the data in question, in particular its massive scale, it would be appropriate for a prior review, if it were required, to be entirely automated. According to that government, such a review, which is of a purely objective nature, is intended essentially to verify that the report referred to Hadopi contains all the required information and data, without Hadopi being required to carry out any assessment of that information or data.

148 However, a prior review may in no case be entirely automated since, as is apparent from the case-law referred to in paragraph 125 above, in the case of a criminal investigation, it is a requirement of such a

review, in any event, that the court or independent administrative body concerned must be able to strike a fair balance between, on the one hand, the legitimate interests relating to the needs of the investigation in the context of combating crime and, on the other hand, the fundamental rights to respect for private life and protection of personal data of the persons whose data are concerned by the access.

149 Such a balancing of the various legitimate interests and rights concerned requires the intervention of a natural person, all the more so where the automatic nature and large scale of the data processing in question poses privacy risks.

150 Furthermore, an entirely automated review is not, as a rule, capable of ensuring that the access does not go beyond the limits of what is strictly necessary and that the persons whose personal data are concerned have effective safeguards against the risks of abuse and against any unlawful access to or use of those data.

151 Thus, while automated reviews may make it possible to verify some of the information contained in the rightholder organisations' reports, such reviews must, in any event, go hand in hand with reviews by natural persons that fully meet the requirements set out in paragraphs 125 to 127 above.

The requirements relating to the substantive and procedural conditions and to the safeguards against the risks of abuse and against any unlawful access to and use of those data applicable to the access by a public authority to data relating to the civil identity associated with an IP address

152 It is apparent from the case-law of the Court that access to personal data can satisfy the requirement of proportionality imposed by Article 15(1) of Directive 2002/58 only if the legislative measure authorising it provides, by means of clear and precise rules, that that access is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abusive or unlawful access to or use of those data (see, to that effect, judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 132 and 173, and of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 49 and the case-law cited).

153 As the Court has pointed out, the need for such safeguards is all the greater where the personal data are subject to automated processing (judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 176 and the case-law cited).

154 In that regard, in reply to a question put by the Court with a view to the hearing on 5 July 2022, the French Government confirmed that, as stated, moreover, by Article L. 331-29 of the CPI, Hadopi's access to data relating to civil identity in the context of the graduated response procedure is the result of essentially automated data processing which is explained by the massive number of instances of counterfeiting detected on peer-to-peer networks by rightholder organisations, which are notified to Hadopi in the form of reports.

155 It is apparent in particular from the documents before the Court that, in the course of that data processing, Hadopi officials check – in an essentially automated manner and without assessing the facts concerned as such – whether the reports referred to that authority contain all the information and data listed in point 1 of the annex to Decree No 2010-236, in particular the factual circumstances attending the illegal making available on the internet concerned and the IP addresses used for that purpose. Such processing must go hand in hand with reviews by natural persons.

156 Since such automated processing is likely to involve a certain number of false positives and, above all, the risk that a potentially very significant amount of personal data may be misused by third parties for unlawful or abusive purposes, it is important that, under a legislative measure, the data processing system used by a public authority is the subject, at regular intervals, of a review by an independent body acting as a third party in relation to that authority, intended to verify the integrity of the system, including the effective safeguards against the risks of abuse and against any unlawful access to or use of those data which that system must ensure as well as the effectiveness and reliability of that system in detecting offending conduct liable to be classified, if repeated, as gross negligence or counterfeiting.

157 Lastly, it must be added that the processing of personal data by a public authority, such as the processing carried out by Hadopi in the context of the graduated response procedure, must comply with the specific rules for the protection of those data laid down by Directive 2016/680, the purpose of which, according to Article 1 thereof, is to lay down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

158 In the present case, even if, under the applicable national law, it does not have decision-making powers of its own, Hadopi, when it processes personal data in the context of the graduated response procedure and adopts measures such as a recommendation or a notification to the person concerned that the conduct in question is subject to criminal prosecution, must be classified as a 'public authority', within the meaning of Article 3 of Directive 2016/680, involved in the prevention, investigation, detection or prosecution of criminal offences, namely the minor offence of gross negligence or the offence of counterfeiting, and therefore falls within the scope of that directive in accordance with Article 1 thereof.

159 In that regard, the French Government stated, in response to a question put to it by the Court with a view to the hearing on 5 July 2022, that since the measures adopted by Hadopi in the context of the graduated response procedure 'are of a pre-criminal nature directly linked to the judicial proceedings', the system for the management of measures for the protection of works on the internet, implemented by Hadopi, is subject, as is clear from the case-law of the referring court, to the provisions of national law designed to transpose Directive 2016/680.

160 By contrast, such data processing by Hadopi does not fall within the scope of the GDPR. Article 2(2)(d) of the GDPR provides that that regulation does not apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

161 As the Advocate General observed in point 104 of his Opinion of 27 October 2022, since Hadopi is required to comply with Directive 2016/680 in the context of the graduated response procedure, the persons involved in such a procedure must enjoy a set of substantive and procedural safeguards including the right of access, rectification and erasure of personal data processed by Hadopi and the possibility of lodging a complaint with an independent supervisory authority, followed, where appropriate, by a judicial remedy under the conditions of general law.

162 In that context, it is apparent from the national legislation at issue in the main proceedings that, in the context of the graduated response procedure, more specifically at the time the second recommendation is sent and at the time of the subsequent notification that the conduct found is liable to constitute a criminal offence, the recipient of those communications enjoys certain procedural guarantees such as the right to submit observations, the right to obtain information concerning the offending conduct he or she is alleged to have engaged in and, as regards that notification, the right to request a hearing and to be assisted by counsel.

163 In any event, it is for the referring court to ascertain whether that national legislation provides for all the substantive and procedural safeguards prescribed by Directive 2016/680.

164 In the light of all the foregoing considerations, the answer to the three questions referred for a preliminary ruling is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as not precluding national legislation which authorises the public authority responsible for the protection of copyright and related rights against infringements of those rights committed on the internet to access data, retained by providers of publicly available electronic communications services, relating to the civil identity associated with IP addresses previously collected by rightholder organisations, so that that authority can identify the holders of those addresses – which have been used for activities liable to constitute such infringements – and may, where appropriate, take measures against them, provided that, under that legislation:

– those data are retained in conditions and in accordance with technical arrangements which ensure that the possibility that that retention might allow precise conclusions to be drawn about the private life of those IP address holders, for example by establishing a detailed profile of those persons, is ruled out – which may be accomplished, in particular, by imposing on providers of electronic communications services an obligation to retain the various categories of personal data, such as data relating to civil identity, IP addresses and traffic and location data, in such a way as to ensure a genuinely watertight separation of those different categories of data, thereby preventing, at the retention stage, any combined use of those different categories of data – and for a period not exceeding what is strictly necessary;

– that public authority's access to such data retained separately and in a genuinely watertight manner serves exclusively to identify the person suspected of having committed a criminal offence and is subject to the necessary safeguards to ensure that that access cannot, except in atypical situations, allow precise conclusions to be drawn about the private life of the IP address holders, for example by establishing a detailed profile of those persons, which entails, in particular, that the officials of that authority authorised to have such access are prohibited from disclosing, in any form whatsoever, information on the content of the files consulted by those holders, except for the sole purpose of referring the matter to the public prosecution service, from tracking the clickstream of those IP address holders and, more generally, from using those IP addresses for any purpose other than that of identifying their holders with a view to the potential adoption of measures against them;

– the possibility, for the persons responsible for examining the facts within that public authority, of linking such data with files containing information that reveals the title of protected works the making available of which on the internet justified the collection of IP addresses by rightholder organisations is subject, in cases where the same person again repeats an activity infringing copyright or related rights, to review by a court or an independent administrative body, which cannot be entirely automated and must take place before any such linking, as such linking is capable, in such circumstances, of enabling precise conclusions to be drawn about the private life of the person whose IP address has been used for activities that may infringe copyright or related rights;

– the data processing system used by the public authority is subject at regular intervals to a review, by an independent body acting as a third party in relation to that public authority, intended to verify the integrity of the system, including the effective safeguards against the risks of abusive or unlawful access to or use of those data, and its effectiveness and reliability in detecting potential offending conduct.

Costs

165 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Full Court) hereby rules:

Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union,

must be interpreted as not precluding national legislation which authorises the public authority responsible for the protection of copyright and related rights against infringements of those rights committed on the internet to access data, retained by providers of publicly available electronic communications services, relating to the civil identity associated with IP addresses

previously collected by rightholder organisations, so that that authority can identify the holders of those addresses – which have been used for activities liable to constitute such infringements – and may, where appropriate, take measures against them, provided that, under that legislation:

– **those data are retained in conditions and in accordance with technical arrangements which ensure that the possibility that that retention might allow precise conclusions to be drawn about the private life of those IP address holders, for example by establishing a detailed profile of those persons, is ruled out – which may be accomplished, in particular, by imposing on providers of electronic communications services an obligation to retain the various categories of personal data, such as data relating to civil identity, IP addresses and traffic and location data, in such a way as to ensure a genuinely watertight separation of those different categories of data, thereby preventing, at the retention stage, any combined use of those different categories of data – and for a period not exceeding what is strictly necessary;**

– **that public authority's access to such data retained separately and in a genuinely watertight manner serves exclusively to identify the person suspected of having committed a criminal offence and is subject to the necessary safeguards to ensure that that access cannot, except in atypical situations, allow precise conclusions to be drawn about the private life of the IP address holders, for example by establishing a detailed profile of those persons, which entails, in particular, that the officials of that authority authorised to have such access are prohibited from disclosing, in any form whatsoever, information on the content of the files consulted by those holders, except for the sole purpose of referring the matter to the public prosecution service, from tracking the clickstream of those IP address holders and, more generally, from using those IP addresses for any purpose other than that of identifying their holders with a view to the potential adoption of measures against them;**

– **the possibility, for the persons responsible for examining the facts within that public authority, of linking such data with files containing information that reveals the title of protected works the making available of which on the internet justified the collection of IP addresses by rightholder organisations is subject, in cases where the same person again repeats an activity infringing copyright or related rights, to review by a court or an independent administrative body, which cannot be entirely automated and must take place before any such linking, as such linking is capable, in such circumstances, of enabling precise conclusions to be drawn about the private life of the person whose IP address has been used for activities that may infringe copyright or related rights;**

– **the data processing system used by the public authority is subject at regular intervals to a review, by an independent body acting as a third party in relation to that public authority, intended to verify the integrity of the system, including the effective safeguards against the risks of abusive or unlawful access to or use of those data, and its effectiveness and reliability in detecting potential offending conduct.**

[Signatures]

---

* Language of the case: French.