Reports of Cases

OPINION OF ADVOCATE GENERAL
SZPUNAR
delivered on 28 September 2023 [1]

Case C-470/21

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

(Request for a preliminary ruling from the Conseil d'État (Council of State, France))

(Reference for a preliminary ruling – Processing of personal data and protection of privacy in the electronic communications sector – Directive 2002/58/EC – Article 15(1) – Power of Member States to restrict the scope of certain rights and obligations – Requirement of prior review by a court or an independent administrative body whose decisions are binding – Civil identity data corresponding to an IP address)

I. Introduction

1. At the request of the Grand Chamber, made in application of Article 60(3) of the Rules of Procedure of the Court, the Court decided on 7 March 2023 to refer the present case to the Full Court.

2. By order of 23 March 2023, the Court (Full Court) decided to reopen the oral part of the procedure and invited the interested parties referred to in Article 23 of the Statute of the Court of Justice of the European Union, the European Data Protection Controller (EDPC) and the European Union Agency for Cybersecurity (ENISA), to take part in a new hearing.

3. I had delivered my first Opinion in this case on 27 October 2022, before the oral part of the procedure was closed. This new Opinion therefore gives me the opportunity to develop certain elements of my reasoning in that case on the key issues relating to the retention of and access to personal data.

[1] Original language: French.

II. Legal context

A. European Union law

4. Recitals 2, 6, 7, 11, 22, 26 and 30 of Directive 2002/58/EC[2] state:

‘(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union [(‘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/EC[3]], 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.

…

[2] Directive 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’).

[3] Directive 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).

(22) The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. …

…

(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. …'

5. Under Article 2 of that directive, headed 'Definitions':

'…

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;

(d) "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

…'

6. Article 3 of that directive, headed '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.'

7. 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. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.'

8. Under Article 6 of Directive 2002/58, headed 'Traffic data':

'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.

…'

9. Article 15(1) of that directive, headed 'Application of certain provisions of Directive [95/46]', provides:

'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 [Union] law, including those referred to in Article 6(1) and (2) [TEU].'

B. French law

1. Intellectual Property Code

10. Article L. 331-12 of the code de la propriété intellectuelle (Intellectual Property Code; 'the CPI') provides:

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

11. Article L. 331-13 of the CPI provides:

'[Hadopi] shall:

…

2. Protect [works and subject matter covered by copyright or a related right in electronic communications networks] from infringements of those rights committed in electronic communications networks used for the provision of online public communications services; …'

12. 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.'

13. Article L. 331-17 of the CPI provides:

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

14. 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 preceding paragraph shall receive referrals sent to that 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 June 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.'

15. Article L. 331-24 of the CPI states:

'The Committee for the protection of rights shall act upon referral by sworn and authorised officials … 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 Commission 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.'

16. 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 against signature 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.'

17. Article L. 331-29 of the CPI provides:

'[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 …'

18. Article R. 331-37 of that code 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 [décret n° 2010-236, du 5 March 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du CPI dénommé 'Système de gestion des mesures pour la protection des œuvres sur internet (Decree No 2010-236 of 5 March 2010 on the automated personal data processing system authorised by Article L. 331-29 of the CPI, known as the 'System for the management of measures for the

protection of works on the internet'),[4] ('the Decree of 5 March 2010')], 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.

…'

19. Article R. 335-5 of the CPI provides:

'I.- Where the conditions laid down in paragraph II are met, gross negligence, punishable by the fine laid down for summary offences in class 5, 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.'

20. Article L. 336-3 of that code provides:

'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 …'

[4] JORF, 7 March 2010, text No 19.

2. Decree of 5 March 2010

21. Article 1 of the Decree of 5 March 2010, in the version applicable to the facts in the main proceedings, 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;

…'

22. 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.'

23. The annex to the Decree of 5 March 2010 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 Public Prosecutor's Office:

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 station (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.

…'

3. Post and Electronic Communications Code

24. Article L. 34-1 of the code des postes et des communications électroniques, as amended by Article 17 of Law No 2021-998 of 30 July 2021 (Post and Electronic Communications Code; 'the CPCE'),[5] provides, in paragraph IIa, that:

'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 IIa(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.'

III. The procedure before the Court

25. In response to the invitation addressed to the parties referred to in Article 23 of the Statute of the Court of Justice of the European Union, the applicants in the main proceedings, the French, Danish and Estonian Governments, Ireland, the Netherlands, Finnish and Swedish Governments and the European Commission answered the written questions put by the Court.

26. Those parties, apart from the Finnish Government, and also the Czech, Spanish, Cypriot, Latvian and Norwegian Governments, and the EDPC and ENISA, took part in the hearing on 15 May 2023.

IV. Analysis

27. My analysis of the questions for a preliminary ruling in my first Opinion had led me to propose that the Court should rule that Article 15(1) of Directive 2002/58 must be interpreted as not precluding national legislation which allows providers of electronic communications services

[5] JORF of 31 July 2021, text No 1. That version of Article L. 34-1 of the CPCE, in force since 31 July 2021, was adopted following Decision No 393099 of the Conseil d'État (Council of State) of 21 April 2021 (JORF of 25 April 2021) striking down the previous version of that provision, which included an obligation to retain personal data 'for the purposes of investigating, detecting and prosecuting criminal offences or a failure to fulfil the obligation laid down in Article L. 336-3 [of the CPI]' with the sole aim of making information available, as necessary, to Hadopi, among others. By Decision No 2021-976-977 QPC of 25 February 2022 (*Mr Habib A. and Another*), the Conseil constitutionnel (Constitutional Council, France) declared that earlier version of Article L. 34-1 of the CPCE to be contrary to the French Constitution, essentially because, 'by authorising the general and indiscriminate retention of connection data, the contested provisions disproportionately interfere with the right to respect for private life' (paragraph 13). The Conseil constitutionnel (Constitutional Council) considered that the connection data which had to be retained under those provisions not only related to the identification of users of electronic communications services, but also covered other data which, 'in view of their varied nature and the processing which they may undergo … provide extensive and specific information on those users and, in some circumstances, on third parties, which is especially detrimental to their privacy' (paragraph 11).

to retain, and an administrative authority such as Hadopi [6] to access, data which are limited to civil identity data corresponding to IP addresses, so that that authority can identify the holders of those addresses suspected of having committed infringements of copyright and related rights and, if appropriate, take action against them, where that access is not subject to a prior review by a court or an independent administrative body, provided that those data are the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the infringement to be identified.

28. In this Opinion, I shall endeavour to develop certain elements of my earlier analysis and the points discussed at the hearing on 15 May 2023, in order to explain the reasons why I maintain both my proposed answer to the questions for a preliminary ruling and the reasoning that led me to that answer. [7]

29. More particularly, I shall demonstrate that the fact of permitting the retention of and access to civil identity data corresponding to IP addresses, without a prior review, in order to identify the perpetrators of infringements when those data are the only means of identifying those persons satisfies the requirements laid down by the Court concerning the examination of measures taken on the basis of Article 15(1) of Directive 2002/58 (Section B).

30. In doing so, I shall show that such a solution amounts not to a departure from the strict case-law on the protection of fundamental rights that has been developed by the Court since the judgments in *Tele2 Sverige and Watson and Others* [8] and *La Quadrature du Net and Others*, [9] but a necessary development of that case-law which, in my view, is part of the extension of the principles laid down by the Court. That distinction is not merely semantic: the solution which I propose aims not to call in question the existing case-law, but, with a view to a certain pragmatism, to enable that case-law to be adapted in particular and very narrowly defined circumstances (Section C).

31. In the interest of clarity, and in so far as the discussions at the hearing demonstrated a need for clarification in that respect, I shall begin my analysis by describing the functioning of the graduated response mechanism operated by Hadopi (Section A).

A. The graduated response mechanism operated by Hadopi

32. Hadopi is an independent administrative authority responsible for protecting copyright and related rights against infringements of those rights committed on the internet. For that purpose, what is known as the 'graduated response' mechanism, the implementation of which is entrusted to Hadopi's Commission for the protection of rights, was introduced.

6 On 1 January 2022, the Conseil supérieur de l'audiovisuel (Higher Audiovisual Council, France) (CSA) and Hadopi became the Autorité de régulation de la communication audiovisuelle et numérique (Authority for the Regulation of Audiovisual and Digital Communications, France) (Arcom). In view of the period during which the facts of the dispute in the main proceedings occurred, I shall, however, refer in this Opinion to Hadopi.

7 In that regard, I also adhere to my proposal that the questions for a preliminary ruling should be reformulated, and also to my understanding of their purpose. While the wording of the questions mentions only access to civil identity data corresponding to IP addresses, the question of access to those data cannot be separated from the question of their retention by the electronic communications providers, and the analysis of the compatibility with EU law of the retention of those data is therefore a necessary prerequisite of the analysis of the compatibility of access to the data. See, on that point, point 45 et seq. of my first Opinion. Likewise, although the questions refer to 'civil identity data corresponding to an IP address', they must be understood as also referring to access to IP addresses that allow the source of a connection to be identified. See, on that point, point 41 et seq. of my first Opinion.

8 Judgment of 21 December 2016 (C-203/15 and C-698/15, 'the judgment in *Tele2*', EU:C:2016:970).

9 Judgment of 6 October 2020 (C-511/18, C-512/18 and C-520/18, 'the judgment in *La Quadrature du Net and Others*', EU:C:2020:791).

33. That Commission receives referrals from rightholder organisations, within which certain sworn officials approved by the Minister for Culture collect, on peer-to-peer networks, the IP addresses of internet users who make works available to the public without the authorisation of their holders. Reports are then prepared. They contain, inter alia, the IP address of the internet access used to commit those infringements of copyright, the date and time of the infringement recorded and the title of the work in question, and are sent to Hadopi's Commission for the protection of rights. It should be emphasised, in that regard and as the EDPC has pointed out, that the processing of personal data by the officials within the rightholder organisations is authorised by the Commission nationale de l'informatique et des libertés (CNIL), the French data protection regulatory authority. [10]

34. Upon receipt of those reports, and following an automated check to ensure that they contain all necessary data, Hadopi's Commission for the protection of rights may obtain from the electronic communications service provider the identity, postal address, electronic address and telephone number of the holder of the subscription that was used to commit a copyright infringement.

35. Hadopi may then send that person a 'recommendation' informing him or her that his or her internet access has been used in a manner contrary to copyright and ordering the person suspected of having failed to fulfil his or her obligation to exercise due diligence as regards respect on the internet for works protected by copyright or a related right to fulfil that obligation. In other words, the recommendation is sent to the holder of the internet access, who may in fact be a different person from the one who made the work available in breach of copyright. A second recommendation may be issued in the event of a second finding of infringement by means of the same internet access. In the event of fresh repetitions, Hadopi's Commission for the protection of rights may decide to refer the matter to the Public Prosecutor's Office with a view to criminal proceedings being brought. In that regard, as the French Government made clear in its first observations, the Hadopi officials responsible for the graduated response mechanism are sworn officials authorised by the President of Hadopi, they are bound by professional secrecy and they are the only individuals within Hadopi to have access to the personal data processed in the context of that mechanism.

36. I must make clear, in that regard, that the data collected and sent to Hadopi are not the data of all peer-to-peer network users when the users merely download such content [11] but only the data of persons who have made counterfeit content available, that is to say, who have *uploaded* such content.

37. By way of illustration, for 2021, Hadopi thus received almost four million reports from rightholder organisations, it issued 210 595 first recommendations and 53 564 second recommendations and it referred the matter to the Public Prosecutor's Office in 1 484 cases.

38. Having thus described the functioning of that mechanism, I shall show how such a mechanism, which entails the retention of and access to civil identity data corresponding to IP addresses, satisfies in my view the requirements of the case-law relating to national measures adopted under Article 15(1) of Directive 2002/58.

[10] See, in that regard, Deliberation No 2010-225 de la CNIL, of 10 June 2010, amending the authorisation of the implementation by the Société des auteurs compositeurs et éditeurs de musique (Society of Authors, Composers and Publishers of Music, France) (SACEM) of the processing of personal data for the purpose of investigating and establishing counterfeiting offences committed via 'peer-to-peer' file exchange networks (Autorisation No 1425421).

[11] Regarding the operation of peer-to-peer networks and the various profiles of users on those networks, see my Opinion in *M.I.C.M.* (C-597/19, EU:C:2020:1063, point 37 et seq.).

B. Compliance with the requirements arising from the Court's case-law relating to the interpretation of Article 15(1) of Directive 2002/58

39. As I have already reviewed, in my first Opinion, the Court's case-law relating to the retention of and access to the IP addresses assigned to the source of a connection, [12] I shall focus in this Opinion on what to my mind is the heart of that case-law, namely, first, the requirement of proportionality and, second, so far as access to those data is concerned, the possible need for a prior review by a court or an independent administrative authority.

1. The proportionality of the measure at issue

40. In order to determine the compatibility with EU law of a measure providing for the retention of or access to civil identity data corresponding to an IP address, it is necessary, as the Court repeatedly emphasises, to reconcile the various interests and rights at issue, these being, on the one hand, the rights to protection of private life and to protection of personal data [13] guaranteed by Articles 7 and 8 of the Charter and, on the other, protection of the rights and freedoms of others and of the rights enshrined in Articles 3, 4, 6 and 7 of the Charter. [14] I shall add that, in the case which concerns us, the rights to protection of private life and to protection of personal data must be reconciled with the right to property enshrined in Article 17 of the Charter, in that the graduated response mechanism ultimately aims to protect copyright and related rights.

41. The Court makes clear, in that regard, that that reconciliation carried out under Article 15(1) of Directive 2002/58 allows the Member States to adopt a measure derogating from the principle of confidentiality where such a measure is '*necessary, appropriate and proportionate* within a democratic society' (emphasis added). Recital 11 of that directive specifies that a measure of that nature must be 'strictly' *proportionate* to the intended purpose. [15]

42. The Court refers, moreover, to the principle of proportionality throughout its reasoning relating to the interpretation of Article 15(1) of Directive 2002/58 and thus makes that principle the cornerstone of the examination of a national measure relating to the retention of or access to personal data adopted under that provision.

43. A closer reading of that reasoning reveals that the principle of proportionality includes, in the context of Article 15(1) of Directive 2002/58, different aspects relating, first, to the seriousness of the interference with fundamental rights which the retention of or access to traffic data entails and, second, to the necessity of the measure at issue.

44. As regards the retention of, and access by Hadopi to, the civil identities corresponding to IP addresses by Hadopi, I am of the view that both the seriousness of the interference and the indispensable nature of those data should lead the Court to adjust its examination of the proportionality of a national measure adopted under Article 15(1) of Directive 2002/58.

[12] Point 53 et seq. of my first Opinion.

[13] The rights to protection of private life and to the protection of personal data are reflected, in the context of Directive 2002/58, in the principles of confidentiality of communications and the prohibition on the storage of the data relating to those communications which it establishes.

[14] Judgments in *La Quadrature du Net and Others* (paragraphs 120 to 122, 127 and 128); of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, 'the judgment in *Commissioner of An Garda Síochána and Others*', EU:C:2022:258, paragraphs 48 and 50); and of 20 September 2022, *SpaceNet and Telekom Deutschland* (C-793/19 and C-794/19, 'the judgment in *SpaceNet and Telekom Deutschland*', EU:C:2022:702, paragraphs 63 and 65).

[15] Judgments in *La Quadrature du Net and Others* (paragraph 129); in *Commissioner of An Garda Síochána and Others* (paragraph 51); and in *SpaceNet and Telekom Deutschland* (paragraph 66).

(a) The relative seriousness of the interference with fundamental rights

45. It is clear from the Court's consistent case-law that, in accordance with the principle of proportionality, the importance of the objective pursued by a measure adopted under Article 15(1) of Directive 2002/58 must be proportionate to the seriousness of the interference that it entails. [16]

46. More particularly, the Court has held, as I emphasised in my first Opinion, that a serious interference may be justified, in the area of prevention, investigation, detection and prosecution of criminal offences, only by the objective of combating crime, which must also be classified as 'serious'. [17]

47. As regards the IP addresses, the Court observes that although they are less sensitive than other traffic data, the retention and analysis of those IP addresses nonetheless constitute serious interferences with fundamental rights, since they may be used for exhaustive tracking of an internet user's clickstream and, therefore, to produce a detailed profile of the user and to draw precise conclusions about his or her private life. [18]

48. In the main proceedings, the purpose of the retention of and access to civil identity data corresponding to IP addresses is to combat infringements of copyright and related rights. To my mind, combating infringements of copyright clearly cannot be classified as combating serious crime, [19] even though the volume of copyright infringements is huge. There is thus a discrepancy between the seriousness of the interference with fundamental rights which the measure at issue entails and the objective which it pursues.

49. In my first Opinion, I considered, in accordance with the Court's case-law, that Hadopi's access to the civil identity data corresponding to an IP address does indeed constitute a serious interference with fundamental rights. Although I also considered that the retention of and access to those data should nonetheless be allowed in the present case, I find it necessary, in the wake of the hearing, to explain further.

50. The graduated response mechanism allows Hadopi to link the IP address communicated by the rightholder organisations of persons suspected of having used their internet access to commit an infringement of copyright on a peer-to-peer network with the civil identity of that person, and also an extract from the file uploaded in breach of copyright. As the Commission and the EDPC observed at the hearing, while such elements no doubt make it possible to obtain more information than just the identity of the presumed perpetrator of an infringement, they do

[16] Judgments in *Commissioner of An Garda Síochána and Others* (paragraph 56), and in *SpaceNet and Telekom Deutschland* (paragraph 71).

[17] Judgments in *Tele2* (paragraph 115); of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788, paragraph 56); and of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications*) (C-746/18, 'the judgment in *Prokuratuur*', EU:C:2021:152, paragraph 33). See also point 92 of my first Opinion.

[18] See judgments in *La Quadrature du Net and Others* (paragraphs 152 and 153); in *Commissioner of An Garda Síochána and Others* (paragraph 73); and in *SpaceNet and Telekom Deutschland* (paragraph 103). See also points 63, 64 and 93 of my first Opinion.

[19] I maintained, in my first Opinion, that the concept of 'serious crime' must be given an autonomous interpretation, in order to prevent Member States from circumventing of the requirements laid down in Article 15(1) of Directive 2002/58. I maintain that position. I must emphasise, however, that even if the Court should find that the definition of 'serious crime' is to be left to the Member States, that definition should in any event be established within the limits of EU law and could not be extended to the point of depriving that provision of its essence.

not result in very precise conclusions about that person's private life being drawn. As I had stated in my first Opinion,[20] all that is revealed is a specific viewing of content which, taken on its own, does not enable a detailed profile of the person who viewed the content to be produced.

51. That applies a fortiori because, first of all, the great majority of the IP addresses communicated by Hadopi are so-called dynamic IP addresses, which by nature change and correspond to a specific identity only at a single moment, which coincides with the making available of the content in question. They therefore preclude any exhaustive tracking.

52. Next, I must emphasise that the protection of fundamental rights on the internet does not in my view justify access to the data relating solely to the IP address, the content of a work and the identity of the person who made it available in breach of copyright not being permitted, but means only that the retention of and access to those data must be accompanied by guarantees. To my mind, an analogy with the real world is telling: a person suspected of having committed theft cannot rely on his or her right to protection of his or her private life to prevent those responsible for prosecuting that offence from ascertaining what the content stolen is. On the other hand, that person may rightly rely on his or her fundamental rights to ensure that, during the proceedings, access will not be provided to more extensive data than just the data necessary for the classification of the alleged offence.

53. Last, I observe that, contrary to the applicants' claims, the graduated response mechanism does not appear to entail the general surveillance of users of peer-to-peer networks. That procedure does not involve monitoring their entire activity on a given network in order to determine whether they have made a work available in breach of copyright, but rather determining, on the basis of a file identified as counterfeit, the holder of the internet access through which the user made the content available. Likewise, as the EDPC emphasised at the hearing, it is not a question of monitoring the activity of all users of peer-to-peer networks, but only that of persons uploading infringing files, as the uploading of those files reveals much less information about the person's private life because files may be uploaded for the sole purpose of enabling those users then to download other files.

54. In those circumstances, the reasons that have led the Court to consider the retention of and access to IP addresses to be a serious interference with fundamental rights do not seem to me to be applicable in the case of a graduated response mechanism such as that operated by Hadopi. It follows that the seriousness of the interference which the retention of and access to those data entail should, in the examination of the principle of proportionality, be nuanced.

55. In other words, I am of the view that the Court's case-law relating to the seriousness of the interference with fundamental rights caused by the retention of and access to IP addresses should be interpreted as meaning not that that interference is always a serious interference, but that it is a serious interference only where the IP addresses may result in the exhaustive tracking of the user's clickstream and in very precise conclusions being drawn about his or her private life.

56. As that is not the case in a situation such as that at issue in the main proceedings, it follows that the interference which the retention of and access to the civil identities corresponding to an IP address used for the purpose of making available content in breach of copyright entails should be capable of being justified by an objective of combating crime in a broader sense than just serious crime.

[20] Point 101 of my first Opinion.

57. I would observe, moreover, that the interference with fundamental rights entailed by the retention of and access to civil identity data corresponding to an IP address in a situation such as that at issue in the main proceedings is not aggravated by the fact that the holder of the internet access used for the purpose of making infringing content available is not necessarily at the origin of the making available of that content, so that the recommendation sent by Hadopi might lead to the content to which a third party may have had access being revealed to the holder of the internet access. First, I recall that the infringement investigated by Hadopi is that of failure to fulfil the obligation to ensure that access is not used for the purposes of making content available in breach of copyright. It is therefore necessary that the information permitting its classification be sent to the presumed infringer. Second, as I have already stated, I am of the view that the information relating to the work in question does not allow precise conclusions to be drawn about the private life of the person at the origin of its being made available. The fact that that information may be sent to the holder of the internet connection therefore does not go beyond what is necessary to permit the prosecution of the infringement of copyright in question.

(b) The indispensable nature of the data at issue for the detection and prosecution of an infringement

58. In order to ensure the proportionality of a measure entailing the retention of and access to traffic data such as civil identity data corresponding to an IP address adopted under Article 15(1) of Directive 2002/58, it is necessary, according to the Court's case-law, that the interference which it entails be limited to what is strictly necessary to permit the attainment of the objective pursued.[21] That seems to me to be precisely the case so far as the measure at issue in the main proceedings is concerned.

59. As I emphasised in my first Opinion,[22] it follows from the actual case-law of the Court that, where an offence is committed exclusively online, such as an infringement of copyright on a peer-to-peer network, the IP address may be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the infringement to be identified.[23] It follows, in my view, that the retention of and access to the civil identity data corresponding to the IP addresses for the purpose of the detection and prosecution of infringements of copyright committed online are, in accordance with the case-law, strictly necessary for the attainment of the objective pursued.

60. It is true that any requirement to protect personal data entails a limitation of investigative powers. That follows from the very principle of the reconciliation of opposing interests and such a result cannot, as such, be disputed. However, where the IP address is the only means of identifying the person suspected of having committed an online infringement of an intellectual property right, such a situation is distinguished from most criminal prosecutions, in relation to which the Court observes that 'the effectiveness … generally depends not on a single means of investigation but on all the means of investigation available to the competent national authorities for those purposes'.[24] If it were accepted that the civil identity data corresponding to IP addresses must not be retained and accessible in a situation such as that at issue in the main proceedings,

21 Judgments in *La Quadrature du Net and Others* (paragraphs 120 to 122 and 132); in *Commissioner of An Garda Síochána and Others* (paragraphs 48 and 54); and in *SpaceNet and Telekom Deutschland* (paragraphs 63 and 69).

22 Point 78 of my first Opinion.

23 Judgments in *La Quadrature du Net and Others* (paragraph 154); in *Commissioner of An Garda Síochána and Others* (paragraph 73); and in *SpaceNet and Telekom Deutschland* (paragraph 100).

24 Judgment in *Commissioner of An Garda Síochána and Others* (paragraph 69).

that, like any measure ensuring the protection of traffic data, would not lead to a mere limitation of the investigative powers, but would indeed deprive the national authorities of the only means of detection and prosecution of certain offences.

61. In other words, it is not a question, according to the interpretation of Article 15(1) of Directive 2002/58 which I propose, of permitting, by means of the examination of the necessity for such a measure, the retention of and access to data that merely *facilitate* the detection and prosecution of infringements, where those infringements may also be detected and prosecuted by competing, even less efficient, means. It is, on the contrary, a question of permitting the retention of and access to those data where they are *indispensable* for the identification of the person suspected of having committed an infringement, who could not be prosecuted without those means, since the data in question constitute the only means of identifying the user in so far as the infringement is implemented exclusively online.

62. Such an interpretation is in my view inevitable, unless it is accepted that a whole range of criminal offences may evade prosecution entirely. [25]

63. It follows from all of the foregoing that to my mind national legislation which permits the retention by providers of electronic communications services of, and access by an administrative authority to, civil identity data corresponding to IP addresses is wholly proportionate to the objective pursued, namely the prosecution of infringements of copyright and related rights on the internet, in so far as the interference with fundamental rights which they entail is of limited seriousness and in so far as those data are the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the infringement to be identified.

64. I am therefore of the view that Article 15(1) of Directive 2002/58 should be interpreted as not precluding such legislation.

2. The existence of adequate material and procedural guarantees

65. As regards, specifically, access to civil identity data corresponding to IP addresses, it follows from the Court's case-law that the strict proportionality of the measure is not in itself sufficient to render it compatible with Article 15(1) of Directive 2002/58.

66. In order to ensure that access to traffic and location data is limited to what is strictly necessary, the Court has held that that access be subject to a prior review carried out either by a court or by an independent administrative body having all the powers and providing all the guarantees necessary in order to reconcile the various legitimate interests and rights at issue. [26]

67. A strict reading of the case-law would therefore lead to the conclusion that Hadopi's access to the civil identity data corresponding to the IP addresses of persons suspected of having committed an infringement of copyright on the internet should be subject to such a prior review, which is lacking in the graduated response mechanism in its existing form.

[25] Point 81 of my first Opinion. See also, on that point, point 79 et seq. of this Opinion.

[26] Judgments in *Tele2* (paragraph 120); in *Prokuratuur* (paragraphs 51 and 52); and in *Commissioner of An Garda Síochána and Others* (paragraphs 106 and 107).

68. However, I am of the view that, as Ireland submitted at the hearing and as I maintained in my first Opinion, the requirement of a prior review by a court or by an independent administrative body is not a systematic requirement, but depends on a more comprehensive analysis of the measure at issue, in which both the seriousness of the interference which it entails and the guarantees which it provides are taken into account.

69. It must be emphasised that each of the judgments referring to that requirement of a prior review by a court or by an independent administrative body concerned national legislation permitting access to all the traffic and location data of users relating to all the means of electronic communication of users [27] or, at least, to the fixed and mobile telephones [28] of identified users.

70. I infer that the requirement of such a review is guided by the seriousness of the interference at issue in the cases in question. As the Court has made clear, it was a matter of data that were 'indeed liable to allow precise, or even very precise, conclusions to be drawn concerning the private lives of the persons …, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. [29] In addition, the data concerned were those of persons already identified and suspected of having committed an infringement on the basis of other factors, and the data at issue therefore made it possible to strengthen the incriminating evidence against the user in question by extending the scope of the data relating to him or her.

71. As regards the legislation at issue in the main proceedings, and as I have emphasised, the seriousness of the interference entailed by the comparison of a piece of civil identity data and an IP address is indeed less than that resulting from access to a person's entire traffic and location data, in so far as that comparison produces no information allowing precise conclusions about the private life of the person concerned to be drawn.

72. Furthermore, as I observed in my first Opinion, [30] those data relate only to persons who, following an objective report drawn up by the rightholder organisations and recording that the IP address has been used in breach of copyright, have engaged in conduct liable to constitute a failure to fulfil the obligation of vigilance, laid down in Article L.336-3 of the CPI. They are not identified in advance by other means, as the comparison of the IP address with the civil identity data is the only means of identification of the person concerned. Access to those data therefore does not, as was the position in the cases on which the Court has previously had to rule, permit additional precise information to be obtained about the activity of persons already suspected on the basis of other evidence, but only permits the IP address, otherwise of no interest, to be exploited. In those circumstances, the data to which Hadopi has access are de facto limited.

73. There is, in my view, a fundamental difference between having access to personal data relating to a person suspected of having committed an infringement, for the purpose of demonstrating his or her guilt, and allowing the identity of the perpetrator of an infringement which has already been established to be revealed.

27 Judgments in *Tele2* and in *Commissioner of An Garda Síochána and Others*.

28 Judgment in *Prokuratuur*.

29 Judgment in *Prokuratuur* (paragraph 36).

30 Point 102 of my first Opinion.

74. That applies a fortiori, in my view, because the collection of the IP addresses on the peer-to-peer networks is subject to prior authorisation limited solely to those data, so that Hadopi is never in possession of an unlimited set of data in the case of users suspected of having committed an infringement of copyright on the internet. [31]

75. Therefore, the logic which underlies the requirement of a prior review carried out by a court or an independent administrative body is not applicable in the case of the graduated response mechanism such as that at issue in the main proceedings and such a requirement therefore does not seem to me to be necessary in order to ensure that the interference with fundamental rights which that mechanism entails is limited to what is strictly necessary.

76. It follows from all of the foregoing that national legislation permitting the retention of, and access by an independent administrative authority such as Hadopi to, civil identity data corresponding to IP addresses in order to identify the holders of those addresses suspected of being responsible for infringements of copyright, where that access is not subject to a prior review by a court or an independent administrative body ultimately respects the principles laid down in the Court's case-law, where those data are the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the infringement to be identified, and Article 15(1) of Directive 2002/58 should therefore be interpreted as not precluding such legislation.

77. In addition to those considerations, which are specific to the case at issue in the main proceedings, I must make a number of more general remarks on the need to proceed with that development of the Court's case-law.

C. A necessary and limited development of the case-law

78. A number of arguments operate in favour of the refinement of the Court's case-law relating to the retention of and access to data such as the IP addresses linked with civil identity data.

79. In the first place, and as I have already observed, [32] in the situation at issue in the main proceedings, obtaining the civil identity data corresponding to an IP address is the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the infringement to be identified.

80. It necessarily follows that if the Court were led to consider that Article 15(1) of Directive 2002/58 nonetheless precludes the retention of and access to those data, the national authorities would be deprived in practice of that sole means of identification and, consequently, the perpetrators of the infringement in question could never be prosecuted. [33] That led me, in my first Opinion, to raise the possibility of systemic impunity for that infringement. [34]

81. The risk of systemic impunity is not limited to infringements of copyright committed on peer-to-peer networks, but, as the Czech Government submitted at the hearing, extends to all offences exclusively committed online.

[31] Point 33 of this Opinion.

[32] Point 59 of this Opinion.

[33] Point 62 of this Opinion.

[34] Point 78 et seq. of my first Opinion.

82. Where the perpetrator of an offence can be identified solely by means of his or her IP address, that offence could never be prosecuted and the measures which prohibit such offences could never be applied if it were to be held that both the retention of and access to those data are contrary to EU law.

83. In that regard, I note that it is true, as the applicants in the main proceedings have submitted, that other means might permit the identification of the perpetrators of certain offences exclusively committed online. Thus, they refer, in particular, to the identifier used on social networks and to the data associated with the user's account, his or her email address, his or her telephone number, or an element of his or her private life which the person would have revealed. However, such data require, for the purpose of connecting them with the person's identity, detailed investigations, in the course of which the user's online activity is examined. The use of such means of investigation therefore seems to me to be capable, unlike the IP address alone, of allowing very precise conclusions to be drawn about the persons' private life, so that the retention of and access to those data would, in that sense, be contrary to Article 15(1) of Directive 2002/58.

84. In those circumstances, access to civil identity data corresponding to a user's IP address is indeed not the only theoretical means of investigation enabling the person to whom that address was assigned at the time of the commission of the infringement to be identified, but is the means enabling the infringement to be prosecuted while entailing the least interference with that person's fundamental rights and, consequently, of precluding general impunity.

85. In the second place, I again emphasise that such a solution makes it possible, in my view, to reconcile two lines of authority in the Court's case-law, the sources of a certain tension which I had identified in my first Opinion [35] and in my Opinion in *M.I.C.M.*, [36] namely, on the one hand, the case-law relating to the retention of and access to the data and, on the other, the case-law relating to the disclosure of the IP addresses assigned to the source of a connection in actions to enforce the protection of intellectual property rights brought by private individuals.

86. In the third place, while the Court's case-law since the judgments in *Tele2* and in *La Quadrature du Net and Others* must be welcomed in that it has enabled a framework that protects the fundamental rights of users of electronic communications services to be put in place, it nonetheless bears the hallmarks of a somewhat case-by-case approach. In the course of dealing with the cases referred to it, the Court has progressively refined its case-law in a way that has allowed it to examine various national legislative provisions in the light of Article 15(1) of Directive 2002/58. However, it is impossible for the Court to predict virtually all the measures that might be the subject of an analysis in the light of that provision. That is evidenced by the number of references for a preliminary ruling [37] of which that provision has formed the subject

[35] Point 69 et seq. of my first Opinion.

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

[37] Judgments of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788); in *La Quadrature du Net and Others*; in *Prokuratuur*; in *Commissioner of An Garda Síochána and Others*; and in *SpaceNet and Telekom Deutschland*.

matter since the judgment in *Tele2*, which in my view attests to the difficulty which the national courts may experience in applying the principles laid down in the Court's case-law to situations that differ from those that gave rise to the judgments in question. [38]

87. It therefore follows that a certain flexibility seems to me to be called for when measures which could not be envisaged at the time of previous judgments are examined by the Court, such as legislation aimed at offences which can be prosecuted only in so far as the civil identity data corresponding to IP addresses are retained and accessible, in respect of which the Court has thus far not been required to rule.

88. It is therefore not a matter, as the Danish Government had argued, of reconsidering the Court's case-law, but of accepting that, on the basis of the principles that underlie that case-law, a more nuanced solution might be identified, in very limited circumstances.

89. The interpretation of Article 15(1) of Directive 2002/58 which I propose permits the retention of and access to civil identity data corresponding to IP addresses only with respect to the prosecution of infringements the perpetrators of which could not be identified in the absence of those data. It therefore covers only infringements committed exclusively on the internet and does not call in question the solutions laid down in the case-law relating to the retention of and access to a wider range of data, and pursuing other objectives.

V. Conclusion

90. In the light of all of the foregoing considerations, I propose that the Court should answer the questions for a preliminary ruling referred by the Conseil d'État (Council of State, France) as follows:

Article 15(1) of Directive 2002/58/CE 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 of Article 52(1) of the Charter of Fundamental Rights of the European Union,

must be interpreted as not precluding national legislation permitting the retention by providers of electronic communications services of, and access by an administrative authority entrusted with the protection of copyright and related rights against infringements of those rights committed on the internet to, data limited to civil identity data corresponding to IP addresses so that that authority can identify the holders of those addresses suspected of having committed those infringements and, if appropriate, take action against them, where that access is not subject to a

[38] In that regard, the increase in the number of requests for a preliminary ruling seeking the interpretation of Article 15(1) of Directive 2002/58 may also indicate a certain reluctance of the part of the national courts to applying the principles established by the Court to situations which are slightly different, owing to the specific characteristics of the national legal orders. On that point, see, in particular, Cameron, I., 'Metadata retention and national security: *Privacy international* and *La Quadrature du Net*', *Common Market Law Review*, 2021, Vol. 58, No 5, pp. 1433 to 1471, or Bertrand, B., 'L'audace sans le tact: jusqu'où la Cour de justice peut-elle aller trop loin?', *Dalloz IP/IT*, 2021, No 9, pp. 468 to 472. It therefore seems to me to be all the more essential, from the aspect of maintaining a meaningful dialogue between the Court and the courts of the Member States, that the Court should be able to adapt when the circumstances so dictate. As writers have observed, the high standard of protection established by the Court's case-law cannot be really effective without the commitment of the national courts, which have primary responsibility for implementing it. On that point, see, among others, Teyssedre, J., 'Strictly regulated retention and access regimes for metadata: *Commissioner of An Garda Siochana*', *Common Market Law Review*, Vol. 60, No 2, 2023, pp. 569 to 588, and Sirinelli, J., 'La protection des données de connexion par la Cour de justice: cartographie d'une jurisprudence européenne inédite', *Revue trimestrielle de droit européen*, Vol. 57, No 2, 2021, pp. 313 to 329.

prior review by a court or an independent administrative authority, provided that those data are the only means of investigation enabling the persons to whom that address was assigned at the time of the commission of the infringement to be identified.