Reports of Cases

Case C-470/21

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

(Request for a preliminary ruling from the Conseil d'État (France))

Judgment of the Court (Full Court) of 30 April 2024

(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)

1. *Protection of natural persons with regard to the processing of personal data – Regulation 2016/679 – Concept of the processing of personal data – Collection, by rightholder organisations, of IP addresses of users of a peer-to-peer network for the purposes of their use in administrative or judicial proceedings – Included*
(European Parliament and Council Regulation 2016/679, Arts 4(2) and 6(1), first subpara., point (f))

(see paragraphs 54, 60-62)

2. *Approximation of laws – Telecommunications sector – Processing of personal data and the protection of privacy in the electronic communications sector – Directive 2002/58 – Scope –Matching, by providers of electronic communications services, of collected IP addresses*

with the holders of those addresses, for the purposes of the use of those data in administrative or judicial proceedings – Included
(European Parliament and Council Directive 2002/58, as amended by Directive 2009/136, Art. 3)

(see paragraphs 55, 63)

3. *Approximation of laws – Telecommunications sector – Processing of personal data and the protection of privacy in the electronic communications sector – Directive 2002/58 – Power of Member States to limit the scope of certain rights and obligations – National legislation providing for the general and indiscriminate retention of data relating to the civil identity associated with IP addresses – Objective of combating criminal offences in general – Whether permissible – Conditions – Obligation for a Member State to lay down strict requirements relating to the arrangements for the retention of those data*
(Charter of Fundamental Rights of the European Union, Arts 7, 8, 11 and 52(1); European Parliament and Council Directive 2002/58, as amended by Directive 2009/136, Art. 15(1))

(see paragraphs 65-70, 73-93)

4. *Approximation of laws – Telecommunications sector – Processing of personal data and the protection of privacy in the electronic communications sector – Directive 2002/58 – Power of Member States to limit the scope of certain rights and obligations – National legislation allowing a public authority to access data relating to the civil identity associated with IP addresses –Legislation intended to combat infringements of copyright and related rights committed on the internet – Whether permissible – Conditions*
(Charter of Fundamental Rights of the European Union, Arts 7, 8, 11 and 52(1); European Parliament and Council Directive 2002/58, as amended by Directive 2009/136, Art. 15(1))

(see paragraphs 95-104, 110-114, 116-119, 122, 164, operative part)

5. *Approximation of laws – Telecommunications sector – Processing of personal data and the protection of privacy in the electronic communications sector – Directive 2002/58 – Power of Member States to limit the scope of certain rights and obligations – National legislation allowing a public authority to access data relating to the civil identity associated with IP addresses – Legislation intended to combat infringements of copyright and related rights committed on the internet – Requirement of a prior review by a court or an independent administrative body before those data may be accessed – Scope – Manner in which that prior review is to be carried out*
(Charter of Fundamental Rights of the European Union, Arts 7, 8, 11 and 52(1); European Parliament and Council Directive 2002/58, as amended by Directive 2009/136, Art. 15(1))

(see paragraphs 124-143, 145, 146, 148-151, 164, operative part)

6. *Approximation of laws – Protection of natural persons with regard to the processing of personal data in criminal matters – Directive 2016/680 – Scope – Concept of 'public authority' – National authority without decision-making power responsible for sending*

warnings to persons suspected of having committed criminal offences – Included – Applicability of substantive and procedural safeguards
(European Parliament and Council Directive 2016/680, Art. 3)

(see paragraphs 157-163)

Résumé

In recent years, the Court of Justice has been called upon, on several occasions, to rule on the retention of and access to personal data in the field of electronic communications and has consequently established an extensive body of case-law in this area.[1] Ruling on a preliminary ruling from the Conseil d'État (Council of State, France), the Court, sitting as the full Court, develops that case-law by providing clarifications concerning (i) the conditions under which the general retention of IP addresses by providers of electronic communications services cannot be regarded as entailing a serious interference with the rights to respect for private life, to the protection of personal data and to freedom of expression guaranteed by the Charter[2] and (ii) the possibility, for a public authority, to access certain personal data retained in accordance with those conditions, in the context of combating infringements of intellectual property rights committed online.

In the present case, four associations submitted a request to the Premier ministre (Prime Minister, France) seeking the repeal of the decree relating to the automated processing of personal data.[3] As that request was not acted upon, those associations brought an action before the Conseil d'État (Council of State) seeking the annulment of that implicit rejection decision. In their view, that decree and the provisions which constitute its legal basis[4] infringe EU law.

Under French law, 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 authorised – in order to be able to identify those responsible for infringements of copyright or related rights committed online – to access certain data that providers of electronic communications services are required to retain. Those data relate to the civil identity of a person concerned associated with his or her IP address previously collected by rightholder organisations. Once the holder of the IP address used for activities constituting such infringements is identified, Hadopi follows the 'graduated response' procedure. Specifically, it is empowered to send that person two recommendations, which are similar to warnings, and, if the

1 See, inter alia, judgments of 21 December 2016, *Tele2 Sverige et Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970); of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788); of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791); of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152); of 17 June 2021, *M.I.C.M.* (C-597/19, EU:C:2021:492); and of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258).

2 Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union ('the Charter').

3 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).

4 In particular, the third to fifth paragraphs of Article L. 331-21 of the Intellectual Property Code.

activities persist, a letter notifying him or her that those activities are subject to criminal prosecution. Finally, it is entitled to refer the matter to the public prosecution service with a view to the prosecution of that person. [5]

In that context, the Conseil d'État (Council of State) referred questions to the Court concerning the interpretation of the ePrivacy Directive, read in the light of the Charter. [6]

Findings of the Court

In the first place, as regards the retention of data relating to civil identity and the associated IP addresses, the Court states that the general and indiscriminate retention of IP addresses does not necessarily constitute, in every case, a serious interference with the rights to respect for private life, protection of personal data and freedom of expression guaranteed by the Charter.

The obligation to ensure such retention may 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.

Accordingly, a Member State which intends to impose such an obligation on providers of electronic communications services must ensure that the arrangements for the retention of those data are such as to rule out the possibility that precise conclusions could be drawn about the private lives of the persons concerned.

The Court specifies that, to that end, 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. Accordingly, the national rules relating to those arrangements must ensure that each category of data, including data relating to civil identity and IP addresses, is kept completely separate from other categories of retained data and that that separation is genuinely watertight, by means of a secure and reliable computer system. In addition, in so far as those rules provide for the possibility of linking the retained IP addresses with the civil identity of the person concerned for the purpose of combating infringements, 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. The reliability of that separation must be subject to regular review by a third-party public authority. In so far as the applicable national legislation provides for such strict requirements, the interference resulting from that retention of IP addresses cannot be categorised as 'serious'.

[5] With effect from 1 January 2022, Hadopi was merged with the Conseil supérieur de l'audiovisuel (Higher Council for the audiovisual sector) (CSA), another independent public authority, to form the Autorité de régulation de la communication audiovisuelle et numérique (Authority for the Regulation of Audiovisual and Digital Communications) (ARCOM). The graduated response procedure has, however, remained essentially unchanged.

[6] 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) (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) ('the ePrivacy Directive'), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

Consequently, the Court concludes that, in the presence of a legislative framework ensuring that no combination of data will allow precise conclusions to be drawn about the private life of the persons whose data are retained, the ePrivacy Directive, read in the light of the Charter, does not preclude a Member State from imposing an obligation to retain IP addresses, in a general and indiscriminate manner, for a period not exceeding what is strictly necessary, for the purposes of combating criminal offences in general.

In the second place, as regards access to data relating to the civil identity associated with IP addresses, the Court holds that the ePrivacy Directive, read in the light of the Charter, does not preclude, in principle, national legislation which allows a public authority to access those data retained by providers of electronic communications services separately and in a genuinely watertight manner, for the sole purpose of enabling that authority to identify the holders of those addresses suspected of being responsible for infringements of copyright and related rights on the internet and to take measures against them. 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.

In that context, the Court notes inter alia that, even though the freedom of expression and the confidentiality of personal data are primary considerations, 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.

In the same context, the Court also refers to its case-law according to which, as regards the combating of criminal offences infringing copyright or related rights committed online, the fact that accessing IP addresses may be the only means of investigation enabling the person concerned to be identified tends to show that the retention of and access to those addresses is strictly necessary for the attainment of the objective pursued and therefore meets the requirement of proportionality. Moreover, not to allow such access would carry a real risk of systemic impunity for 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 to respect for private life, protection of personal data and freedom of expression is a proportionate measure in the light of the objective of combating criminal offences.

In the third place, ruling on whether access by the public authority to data relating to the civil identity associated with an IP address must be subject to a prior review by a court or an independent administrative body, the Court considers that the requirement of such prior review applies where, within the framework of national legislation, 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. Conversely, that requirement of prior review is not intended to apply where the interference with fundamental rights cannot be classified as serious.

In that regard, the Court states that, where a retention framework which ensures a watertight separation of the various categories of retained data is put in place, access by the public authority to the data relating to the civil identity associated with the IP addresses is not, in principle, subject to the requirement of a prior review. Such access for the sole purpose of identifying the holder of an IP address does not, as a general rule, constitute a serious interference with the abovementioned rights.

However, the Court does not rule out the possibility that, in atypical situations, there is a risk that, in the context of a procedure such as the graduated response procedure at issue in the main proceedings, the public authority may be able to draw precise conclusions about the private life of the person concerned, in particular where that 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, revealing potentially sensitive information about aspects of that person's private life.

In the present case, an IP address holder may be particularly exposed to such a risk when the public authority must decide whether or not to refer the matter to the public prosecution service with a view to the prosecution of that person. 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. The access of the competent authority to all of the data relating to the person concerned collected during the various stages of that procedure may enable precise conclusions to be drawn about the private life of that person. Accordingly, the national legislation must provide for a prior review which must take place before the public authority can link the civil identity data and such a set of data, and before sending a notification letter declaring that that person has engaged in conduct subject to criminal prosecution. That review must, moreover, preserve the effectiveness of the graduated response procedure by making it possible, in particular, to identify cases where the unlawful conduct in question has been again repeated. To that end, 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 cannot automatically be linked, by the persons responsible for the examination of the facts within the competent public authority, with information which the latter already has and which could enable precise conclusions to be drawn about the private life of that person.

Furthermore, as regards the object of the prior review, the Court notes that, where the person concerned is suspected of having committed an offence 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 to draw precise conclusions about the private life of that person. However, even access allowing such precise conclusions to be drawn should be authorised in cases where the person concerned is suspected of having committed an offence considered by the Member State concerned to undermine a fundamental interest of society and which thus constitutes a serious crime.

The Court also states that a prior review may in no case be entirely automated since, in the case of a criminal investigation, such a review requires that a balance be struck between, on the one hand, the legitimate interests relating to combating crime and, on the other hand, respect for private life and protection of personal data. That balancing 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.

Thus, the Court concludes that the possibility, for the persons responsible for examining the facts within that public authority, of linking such data relating to the civil identity of a person associated with an IP address 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. That review 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.

In the fourth and last place, the Court notes that the data processing system used by the public authority must be subject, at regular intervals, to a review by an independent body acting as a third party in relation to that public authority. The purpose of that control is 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.

In that context, the Court observes that, in the present case, the automated processing of personal data carried out by the public authority on the basis of the information relating to instances of counterfeiting detected by the rightholder organisations 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, which explains the need for such a review.

In addition, it adds that that processing must comply with the specific rules for the protection of personal data laid down by Directive 2016/680.[7] In the present case, even if the public authority does not have decision-making powers of its own in the context of the 'graduated response' procedure, it must be classified as a 'public authority' involved in the prevention and detection of criminal offences and therefore falls within the scope of that directive. Thus, the persons involved in such a procedure must enjoy a set of substantive and procedural safeguards referred to in Directive 2016/680; it is for the referring court to ascertain whether the national legislation provides for those safeguards.

[7] 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).