



C/2024/3717

24.6.2024

**Judgment of the Court (Full Court) of 30 April 2024 (request for a preliminary ruling from the Conseil d'État – France) – La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net, French Data Network v Premier ministre, Ministre de la Culture**

**(Case C-470/21, <sup>(1)</sup> La Quadrature du Net and Others (Personal data and action to combat counterfeiting))**

*(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)*

(C/2024/3717)

Language of the case: French

## Referring court

Conseil d'État

## Parties to the main proceedings

*Applicants:* La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net, French Data Network

*Defendants:* Premier ministre, Ministre de la Culture

## Operative part of the judgment

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

must be interpreted as not precluding national legislation which authorises the public authority responsible for the protection of copyright and related rights against infringements of those rights committed on the internet to access data, retained by providers of publicly available electronic communications services, relating to the civil identity associated with IP addresses previously collected by rightholder organisations, so that that authority can identify the holders of those addresses – which have been used for activities liable to constitute such infringements – and may, where appropriate, take measures against them, provided that, under that legislation:

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

<sup>(1)</sup> OJ C 462, 15.11.2021.

- that public authority's access to such data retained separately and in a genuinely watertight manner serves exclusively to identify the person suspected of having committed a criminal offence and is subject to the necessary safeguards to ensure that that access cannot, except in atypical situations, allow precise conclusions to be drawn about the private life of the IP address holders, for example by establishing a detailed profile of those persons, which entails, in particular, that the officials of that authority authorised to have such access are prohibited from disclosing, in any form whatsoever, information on the content of the files consulted by those holders, except for the sole purpose of referring the matter to the public prosecution service, from tracking the clickstream of those IP address holders and, more generally, from using those IP addresses for any purpose other than that of identifying their holders with a view to the potential adoption of measures against them;
  - the possibility, for the persons responsible for examining the facts within that public authority, of linking such data with files containing information that reveals the title of protected works the making available of which on the internet justified the collection of IP addresses by rightholder organisations is subject, in cases where the same person again repeats an activity infringing copyright or related rights, to review by a court or an independent administrative body, which cannot be entirely automated and must take place before any such linking, as such linking is capable, in such circumstances, of enabling precise conclusions to be drawn about the private life of the person whose IP address has been used for activities that may infringe copyright or related rights;
  - the data processing system used by the public authority is subject at regular intervals to a review, by an independent body acting as a third party in relation to that public authority, intended to verify the integrity of the system, including the effective safeguards against the risks of abusive or unlawful access to or use of those data, and its effectiveness and reliability in detecting potential offending conduct.
-