# ECJ Ruled on Data Retention of IP Addresses in Piracy Cases

**Thomas Wahl**

eucrim
European Law Forum: Prevention • Investigation • Prosecution

**News**

**AUTHOR**

**Thomas Wahl**
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2024, Vol. 19(2) eucrim
ISSN: 1862-6947
https://eucrim.eu



In its landmark judgment of 30 April 2024, the ECJ specified the requirements for the access to retained identification data on the basis of IP addresses. With this judgment, the ECJ partly deviates from its strict approach on data retention and admits law enforcement access to identity data in order to combat criminal offences of piracy in the internet. The case is officially referred as C-470/21, *La Quadrature du Net and Others* – *and lutte contre la contrefaçon* and unofficially as "La Quadrature du Net II".

## The complaints before the French courts

The case relates to complaints by four data protection associations before French courts seeking annulment of a French decree that allows data processing operations in favour of or by 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"). These operations are considered necessary to effectively combat copyright offences committed in the internet.

The proceedings in France have two peculiarities: First, the data processing operations are twofold: In a first operation, rightholder organisations collect IP addresses which appear to have been used on peer-to-peer websites to commit offences against the protected works in the internet; after referral of these IP addresses to Hadopi, Hadopi requests the internet service providers to match the IP addresses with civil identity data of its holder (second operation).

The second peculiarity is that these identity data are used by Hadopi for a "*graduated response*" in an administrative procedure: Hadopi first sends "recommendations" to the copyright offender (subscriber), which are similar to warnings; in case of a repetition of the offending conduct detected, Hadopi notifies the subscriber that the conduct is liable to constitute a copyright offence of "gross negligence"; and lastly, Hadopi can refer a case to the public prosecution service of conduct that may constitute such an offence of counterfeiting.

It is also noted that the French decree has not included a prior review by a judge or an authority offering guarantees of independence and impartiality.

## The questions referred by the Conseil d'État

The Conseil d'État, France, asked the ECJ whether the data processing operations are in line with EU law, in particular Art. 15 of Directive 2002/58/EC (Directive on privacy and electronic communications/e-privacy Directive), read in the light of the Charter of Fundamental Rights of the European Union ("the Charter"). Doubts mainly arose as to whether the French legislation falls within one of the exceptions to the ban of the

retention of personal data in a general and indiscriminate manner. Such exceptions were mainly established in the ECJ's judgment of 6 October 2020 in *La Quadrature du Net and Others* (→ eucrim 3/2020, 184-186), in which the ECJ decided, *inter alia*, that a general and indiscriminate data retention regime relating to the *civil identity* of users of electronic communications systems for the purposes of combating crime is not precluded by EU law.

Furthermore, the Conseil d'État referred to the ECJ's judgment in *Tele2 Sverige and Watson* (→ eucrim 4/2016, 164), in which a prior review by a court or an independent administrative authority is requested for the access of retained data by the competent authority. However, the French court also points out that, in the present case, such prior review is nearly impracticable considering the high volume of civil identity data that Hadopi as competent authority collects each year.

### Further background of the case

For more background information, see also the two opinions by Advocate General *Szpunar*, summarised in eucrim 3/2022, 190-191 and eucrim 2/2023, 150. The second opinion had to be issued after the case was referred from the Grand Chamber to the Full Court of the ECJ (i.e., all 27 judges) and the Full Court decided to reopen the oral part of the procedure.

### The ECJ's first approach in the judgment

The ECJ, sitting as Full Court, first reiterates its previous case law on the retention of data relating to civil identity and the associated IP addresses. The ECJ 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, if 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. This could happen, *inter alia*, bylinking those IP addresses with a set of traffic or location data. Accordingly, a Member State can impose a respective obligation of data retention on providers of electronic communications services, but it must implement certain arrangements for the retention of those data ruling out the possibility that precise conclusions could be drawn about the private lives of the persons concerned.

The judges in Luxembourg then specify the requirements necessary for both the *retention of data* and *access to data* relating to civil identity and associated IP addresses retained by providers of electronic communications services.

### Requirements surrounding the retention of data relating to civil identity

With regard to the retention of data, the ECJ requires that national rules provide for the following:

- Ensuring that each category of data, including data relating to civil identity and IP addresses, is kept completely separate from the other categories of data retained;
- Ensuring, from a technical point of view, the genuinely watertight separation of the various categories of retained data, in particular data relating to civil identity, IP addresses, the various traffic data other than IP addresses and the various location data, by means of a secure and reliable computer system;
- Permitting the linking of the retained IP addresses with the civil identity of the person concerned only through the use of an effective technical process which does not undermine the effectiveness of the watertight separation of those categories of data;

- Subjecting the reliability of the watertight separation to regular review by a public authority other than that which seeks to obtain access to the personal data retained by the providers of electronic communications services.

The ECJ clarifies in this context that 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".

### Requirements surrounding access to data relating to the civil identity

As regards access to data, the ECJ requires that the national legislation must prohibit the public officials having access to the data retained in the above-described manner to do the following:

- No disclosure in any form whatsoever of information concerning the content of the files consulted by the IP address holders except for the sole purpose of referring the matter to the public prosecution service;
- No tracking in any way of the clickstream of those holders;
- No use of 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 notably 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.

According to the Court, it is exactly in the context of combating criminal offences infringing copyright or related rights committed online that access to IP addresses may be the only means of investigation enabling the person concerned to be identified. This is why 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.

### The question of (judicial/quasi-judicial) control

With regard to the question of adequate control, the ECJ distinguishes between (1) the requirements of a *prior review* by a court or an independent administrative body *before* a public authority accesses data relating to the civil identity associated with an IP address and (2) the requirements of *control against the risks of abuse* and against any unlawful access to / use of those data as well as of respective substantive and procedural safeguards.

### Prior review by court or independent body

Looking at the prior review, the judges in Luxembourg establish the following principles with regard to civil identity data associated with an IP address:

- Prior review is only necessary if access carries the risk of a serious interference with the fundamental rights of the person concerned; this means if a public authority is able to draw precise conclusions about the private life of that person and/or to establish a detailed profile of that person;

- Conversely, the requirement of prior review is not intended to apply where the interference with fundamental rights cannot be classified as serious;
- If a retention framework is in place that ensures a watertight separation of the various categories of retained data (see above), access by the public authority to the data relating to the civil identity associated with the IP addresses does, as a general rule, not constitute a serious interference with fundamental rights and is therefore not, in principle, subject to the requirement of a prior review.
- However, national rules must provide for a prior review if in atypical situations there is a risk that, in the context of a procedure, the public authority may be able to draw precise conclusions about the private life of the person concerned.

Applying these principles to the concrete case, the judges in Luxembourg identified such a risk if Hadopi must decide whether or not to refer the matter to the public prosecution service with a view to the prosecution of that person. This concerns cases in which a subscriber repeatedly shows an activity of infringing copyright or related rights. This means that a review by a court or an independent administrative body must be incorporated at the third stage of the graduated response procedure. By contrast, it does not apply to the previous stages of that procedure; this is justified, inter alia, because of reasons of practicability.

### Manner of prior review: no automatisation

As regards the manner in which that prior review is to be carried out, the ECJ clarifies that a prior review may in no case be entirely automate. The reason is that, in the case of a criminal investigation, such a review requires a balancing 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.

### Control of abuse and data protection safeguards

As regards the means of control of potential abuses by the public authority, the ECJ requires that the data processing system used by the public authority must be subject, at regular intervals, to a review by an independent body. The purpose of that control is to verify the integrity of the system and the reliability in detecting potential offending conduct.

The ECJ adds that the processing in question must comply with the specific rules for the protection of personal data laid down by Directive 2016/680 (“the “Law Enforcement Data Protection Directive – LED”). In the present case, even if the public authority (Hadopi) 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 the LED. Thus, the persons involved in such a procedure must enjoy a set of substantive and procedural safeguards referred to in the LED. It is for the referring court to ascertain whether the national legislation provides for those safeguards.

### Put in focus

The ECJ seized the opportunity to specify the admitted exceptions for the retention of data if it comes to IP addresses and civil identity data. The ECJ particularly stated that IP addresses constitute traffic data for the purposes of Directive 2002/58, but they are distinct from other categories of traffic data and location data. Hence, it held that data retention in relation to IP addresses is, in principle, far less intrusive into fundamental rights than the other categories of data. This was already indicated in its previous judgments on data retention, in particular the first La Quadrature du Net case (→ eucrim 3/2020, 184-186).

However, the judges in Luxembourg made bluntly clear that they also see risks and strict rules must apply if the data can be used or linked in order to draw precise conclusions about the private life of the persons whose data were concerned, for example by establishing a detailed profile of that person. This consequently leads to a serious interference with the fundamental rights enshrined in Arts. 7 and 8 of the Charter, concerning the protection of the privacy and personal data of those persons, and in Art. 11 of the Charter, concerning their freedom of expression. Here, the national legislator is obliged to provide the necessary arrangements to avoid that such scenarios can emerge.

With regard to control mechanisms, the judges in Luxembourg clarified that a system of two layers is in principle required: prior review by a court or independent administrative body *and* regular oversight by independent bodies (e.g., data protection supervisors) over the public law enforcement authority with regard to integrity and reliability of the used data processing system. Problematic may be that prior review is no longer required in all data retention cases where the ECJ takes account of the collection of mass data by the French anti-piracy authority Hadopi. Here, it follows the AG *Szpunar's* opinion who advocated a "pragmatic adaptation" of the case law on data retention. It remains to be seen whether the solution found for the French case also applies to law enforcement authorities in other EU Member States.

With regard to judicial control, the judges in Luxembourg interestingly made statements on automatization. They deny any computer system who takes automated decisions in a judicial review procedure linked to criminal investigations. This can be interpreted as a first and clear objection against tendencies to introduce "artificial intelligence judges" in standardised data processing operations. If fundamental rights or questions of privacy are at stake, intervention by a natural person ("the human judge") is required (see also → *Marcin Górski*, Why a Human Court?, eucrim 1/2023, 83-88).

### Statements

Nonetheless, media and data privacy advocates reacted on the judgment with disappointment. They see in the judgment a "turning point" and argue that the ECJ has changed its previously fundamental rights-friendly stance on data retention, now even allowing for unprovoked surveillance in the case of copyright infringements.

The German Bar Association (DAV) criticised that the ECJ has now made the access to data by law enforcement authorities subject to a court decision only in exceptional cases.

La Quadrature du Net, one of the civil rights organisations that brought the case to court, commented : "The CJEU has considerably watered down its previous case law, with impacts beyond the Hadopi case. With this new ruling, access to IP addresses is no longer considered a serious interference with fundamental rights by default. As a result, the Court allows the possibility of mass surveillance of the Internet.[...] More generally, this decision from the CJEU has, above all, validated the end of online anonymity."

## About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union