ELB Blogpost 50/2023, 4 December 2023
Tags: Case C-470/21, La Quadrature du Net, HADOPI, Data Retention
Topics: HADOPI, Data Retention

A complete U-turn in jurisprudence: *HADOPI* and the future of the CJEU's authority

By Chloé Berthélémy, Jesper Lund and Bastien Le Querrec

This blogpost only reflects the views of their authors and not the organisations they represent.

Introduction

In his second Opinion on the *HADOPI* case (C-470/21) (short for: *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet*), the Advocate General Szpunar seemingly suggests that the Court of Justice of the European Union (CJEU) should change its jurisprudence when Member States refuse to apply it. He argues that the CJEU should be "pragmatic" and "nuanced" when national courts fail to implement its case law. This blog post argues that, if followed by the Court, the interpretation proposed by the AG would lead to a severe weakening of the CJEU's authority and legitimacy, more generally. This would be of great symbolic significance in an already challenging environment for the Court which is faced with increasing defiance of Member States in the field of data protection.

The case, brought by the digital rights group, La Quadrature du Net, questions the compatibility of the "HADOPI" law, the French legal framework to combat the online exchange of copyrighted material without permission from right-holders, with European Union law. After a Grand Chamber hearing in July 2022 and a first AG Opinion in October 2022, the case was referred to the Full Court in March 2023 at the request of the Grand Chamber, pursuant to Article 60(3) of the Rules of Procedure of the Court. A reassignment from the Grand Chamber to the Full Court is very rare, but no reason has been provided in the public documents of the case. A second hearing was held in May 2023, and the AG delivered a second Opinion on 28 September 2023.

The French HADOPI system, named after the administrative authority that oversees it, consists of identifying and sanctioning internet subscribers whose connection has been used to share copy-righted material on peer-to-peer networks. Upon receiving complaints from right-holders or their representatives, the HADOPI authority sends automated requests (AG Opinion, para. 34) to internet service providers (ISPs) to provide civil identity data, email and postal addresses for the user of the IP addresses implicated in infringement(s). The ISP identifies the user by querying a large database of previously assigned source IP addresses linked to user identity. This database is only available because of the French data retention law. The HADOPI system is labelled as a "graduated response" system because the authority first sends two formal warnings to individuals engaged in infringements before resorting to legal action upon detecting a third violation. Access to traffic data by HADOPI is extensive; for example, in 2021, it received four million complaints from right-holders. This means that the HADOPI received and accessed four million of source IP addresses of users accused of illegally sharing protected materials, that is to say, a very large amount of traffic data. However, it decided to refer only 1,484 cases to the public prosecutor (AG Opinion, para. 37).

This post will argue that the HADOPI system is contrary to the Court's extensive data retention case law on two counts. First, the HADOPI system operates by relying on automated access to traffic data, which under the Court's current case law (discussed further below) can only be retained for the purpose of combatting serious crime. Even the AG agrees that copyright infringements clearly cannot be classified as a serious crime (para. 38 of the Opinion). Secondly, the massive access to this traffic data takes place without prior authorisation from a national court or an independent administrative authority.

In his two Opinions, AG Szpunar presents a very different analysis of the case. He concludes that the HADOPI is compatible with EU law. In doing so, he proposes a revision – in his words, a "development" (para. 30 of the second Opinion) – of the Court's case law on data retention in the online sphere, which will have wide-ranging consequences for the privacy and data protection of everyone using the internet.

Existing case law on retention of source IP addresses

In *La Quadrature du Net and Others*, the Court previously made the following proportionality assessment: it held that retention of traffic data constitutes a particularly serious interference with the fundamental rights enshrined in Articles 7, 8 and 11 of the EU Charter of Fundamental Rights. Therefore, data retention and access are only allowed in a targeted manner and for the objective of combatting serious crime (para. 147). The CJEU made an exception for IP addresses assigned to the source of an internet connection ("source IP addresses") that it considered less sensitive than other traffic data and sometimes the only means of investigations for some crimes

committed online (paras. 152-156). Source IP addresses can thus be retained for all users for a period strictly limited to what is necessary. However, in light of the seriousness of the interference of retaining IP addresses about all users without any link to criminal offences, not even an indirect one, only serious crimes and a genuine, present or foreseeable threat to national security can justify the general and indiscriminate retention of source IP addresses.

The HADOPI obtains access to the identity of the subscriber to which a source IP address was assigned at the time of the alleged copyright infringement. While the information disclosed is civil identity data, the disclosure process involves linking the IP addresses collected by right-holders with source IP addresses retained by ISPs. Therefore, the disclosure must be seen as access to source IP addresses which have been retained for the purpose of combatting serious crime. The AG agrees with this assessment (paras 43-44 of the first Opinion). Under the Court's established case law, access to retained traffic data can only be justified by the objectives for which the providers were ordered to retain that data (see *La Quadrature du Net and Others*, para. 166).

Assessment of the AG's proposal

In his second Opinion, the AG takes the opportunity to develop his analysis in the first Opinion of the proportionality of the retention of and access to civil identity data corresponding to IP addresses when investigating and prosecuting crime.

AG Szpunar rejects the conclusion that the HADOPI system involves unlawful access to source IP addresses retained for combatting serious crime. Instead, he proposes to expand the conditions for general and indiscriminate retention of source IP addresses to include all cases where access to such data is the only means of investigation, including the prosecution of ordinary crimes (para. 56). In his first Opinion, this expansion of the purpose for retention was justified by the risk of systemic impunity for offences committed exclusively online (paras 80-81). In his second Opinion, the AG now adds that the retention of and access to source IP addresses should only be considered a serious interference where the source IP addresses may result in exhaustive tracking of the user's clickstream and allow very precise conclusions to be drawn about his or her private life (para. 55). In his view, this is not the case in the situation of access by the HADOPI. The main rationale of the AG is that the HADOPI system only involves a limited subset of the user's internet activity, and that the operation of the system therefore does not constitute a serious interference (paras 50-57).

In this context, it is important to recognise that, in most situations, access to retained source IP addresses by public authorities only involves a small subset of the retained data, namely the identity of the user of an IP address at a specific timestamp. Taken in isolation, access to this small subset of data may not constitute a serious

interference. However, access to such data is only possible because source IP addresses have been retained in a general and indiscriminate manner for a longer period (one year in France), as the timestamps for which access to subscriber identity is sought are obviously not known in advance This retention is a serious interference, as held in *La Quadrature du Net and Others* (paras 152-156), inter alia because the data can be used for exhaustive tracking and because users are entitled to expect to browse the internet anonymously (para. 109). The interference that the access entails must be viewed in light of the retention scheme that makes the access possible. Indeed, a limitation to combatting serious crime at the retention stage because of the seriousness of the interference will be deprived of any practical effect if the retained data can nonetheless be accessed for minor offences (*Commissioner of An Garda Síochána*, para. 98). On this point, even the AG agrees that copyright infringements clearly cannot be classified as a serious crime (para. 38 of the Opinion).

When the AG concludes that source IP addresses processed in the "graduated response" mechanism do not allow for exhaustive tracking because dynamic IP addresses change frequently (para. 51), he is clearly referring to the IP addresses collected by right-holders and communicated to the HADOPI. However, the relevant yardstick must be the IP addresses retained by ISPs because HADOPI is seeking access to that data. For this (much larger) pool of IP addresses, general and indiscriminate retention is a serious interference, as established in *La Quadrature du Net and Others* (paras 152-156).

The risks of weakening the CJEU case law

By permitting general and indiscriminate retention of source IP addresses in *La Quadrature du Net and Others*, the Court sought to strike a balance between the fundamental rights of internet users and the public interest in prosecuting serious offences committed online, where access to retained source IP addresses might be the only means of investigating crimes. The essence of the AG's second Opinion in the *HADOPI* case is that general and indiscriminate retention of source IP addresses, and access to such data, should be considered proportionate and permissible for the purpose of combatting *any offence* committed online. As a consequence, if the AG's Opinion were followed, the balance struck by the Court in *La Quadrature du Net and Others* would be fundamentally altered. No distinction would be made between serious offences like sexual violence against children, and minor offences such as online defamation. People could no longer expect to browse the internet anonymously without the risk of their identity being regularly disclosed to law enforcement in a context where more and more peaceful protest and speech is being criminalised (e.g., crackdowns on climate activists and, more recently, support of Palestinians in Gaza). This would run the risk of having a chilling effect on the exercise of fundamental rights, including freedom of expression and access to information in the online environment (*La Quadrature Du Net and Others*, para. 118); for example, through the use of social media for organising demonstrations and any other form of assembly.

The AG only considers the risk of impunity (para. 81) and minimises the gravity of the interference when internet users can be identified by public authorities without any threshold for wrongdoing (para. 84). In the case of the HADOPI, the identification of the user through the association of the civil identity and the IP address is also associated with the content of a private communication: HADOPI gets access to an extract of the digital file shared online, which discloses the nature and content of the copyrighted material exchanged. Such information is liable to reveal potentially very intimate details about the user, such as political opinions, religious beliefs, and sexual orientation and practices, etc. – data that EU law recognises as particularly sensitive. This has the potential of representing an even greater interference than the already serious breach of data protection caused by the linking of an IP address and civil identity data. The AG tries to downplay that risk with the argument that users may upload certain files to be allowed to download others (certain peer-to-peer networks have a rule to maintain a minimum ratio between upload and download volumes) (para. 53). However, sharing ratio requirements are only enforced in some cases, and the situation described by the AG is not a general characteristic of peer-to-peer communities. Instead, there must be a presumption that right-holders transfer personal data to the HADOPI of persons who have a meaningful engagement with the copyrighted work. And, even in cases where internet users may upload files to be able to download others, this in no way removes the possibility, contrary to what the AG implies, that the files uploaded for that purpose may reveal sensitive information about the people who share them.

No requirement of prior review by a court

Access to the retained source IP address data by the HADOPI authority takes places without authorisation from a court or independent administrative body, which is the second reason why the HADOPI system (in our assessment) falls short of the CJEU requirements. In its data retention case law, the Court has always required prior review by a court or an independent administrative body to ensure that the substantive and procedural conditions for granting access to the retained data are fully observed. The AG proposes to dispense with this requirement because the seriousness of the interference is lower than in the cases previously considered by the Court. For the AG, the HADOPI framework offers sufficient safeguards, even though the HADOPI cannot be regarded as an independent authority for authorising its own access (para. 104 of the first Opinion).

The lower seriousness of the interference is also used to justify access to the retained data in the first place, along with the assumption that there are no other means of investigation (para. 70). Even though these assumptions are critical for permitting access, they will not be subject to verification by an independent authority. This is in rather striking contrast with the *La Quadrature du Net and Others* judgment, where

strict compliance with the substantive and procedural conditions for the use of the retained data was emphasised (see para. 155).

"A necessary development of the case-law": the political implications of yielding under the Member States' pressure

The AG ends his second Opinion by justifying his proposed revision of the CJEU case law by framing it as a "necessary" or "nuanced solution" offered to the Member States that wanted the entire data retention case law "reconsidered" (para. 88). Such a major shift in the Court's interpretation would severely weaken the protection afforded by EU law to privacy online in the age of mass surveillance. This would come at a time where the Council and the Commission are attempting to find solutions to overcome the "challenges that law enforcement practitioners face in their daily work in connection to access to data". Their recently set-up High-Level Group "Going Dark" is supposed to publish recommendations for future EU policies, notably on data retention, after summer 2024. A substantial shift in the case law could thus impact the current political debate to the detriment of the protection fundamental rights.

Furthermore, if the Court were to follow the AG's Opinion, consequences would not be merely legal. It would also send a wrong signal about its authority and role in safeguarding fundamental rights. The AG sees the number of references for a preliminary ruling on matters related to data retention as proof that the current interpretation of the Court of Justice is too difficult for national courts to apply (para. 86, second Opinion). He further argues in footnote 38 that "the Court should be able to adapt when the circumstances so dictate" with a view to "be really effective" and to maintain "a meaningful dialogue between the Court and the courts of the Member States". Adopting this reasoning would represent a clear departure from the Court's stance on data retention. It also risks inviting new data retention cases for "reconsideration" from Member States which for more than ten years have unsuccessfully pleaded before the Court of Justice that the general and indiscriminate retention of all traffic data and location data should be permitted for combatting (any form of) crime.

It would also potentially weaken the Court's legitimacy in the EU's legal governance architecture. Since *Digital Rights Ireland and Others* (C-293/12), Member State governments have wilfully refused to apply the Court's case law and persisted in implementing illegal data retention frameworks. The Commission, which is normally tasked to bring errant Member States into line with EU law, has so far avoided to launch infringement procedures, *de facto* making the Court's rulings ineffective. This lack of enforcement undermines the rule of law. If AG Szpunar's proposal to change direction is followed, it is clear that it would have detrimental consequences for fundamental rights and the democratic principles in the EU.