A ‘necessary and limited development’ of the data retention case law, or its death by a thousand cuts? Sitting as a full Court, the ECJ greenlights retention of IP addresses to fight non-serious crime in Case C-470/21 La Quadrature du Net and Others (Personal data and action to combat counterfeiting)

Robinson, G.L.

Computer Law & Security Review 58 (2025) 106178

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

Comment

A 'necessary and limited development' of the data retention case law, or its death by a thousand cuts? Sitting as a full Court, the ECJ greenlights retention of IP addresses to fight non-serious crime in Case C-470/21 *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)*

Gavin Robinson *

Assistant Professor in Criminal Law and Digital Technologies, eLaw – Center for Law and Digital Technologies, Leiden Law School, Leiden University, Steenschuur 25, 2311 ES Leiden, the Netherlands

ARTICLE INFO

Keywords:
European court of justice
Data retention
copyright
IP addresses
Serious crime
La quadrature du net
General and indiscriminate retention
Access to retained Data

ABSTRACT

This case comment analyses Case C-470/21 *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* ('LDQN II'), in which the Court of Justice held that EU law does not preclude national law imposing the general and indiscriminate retention by electronic communications service providers of IP addresses for the subsequent use of the relevant public authorities in the fight against copyright infringements online. In a very rare occurrence, the judgment in *LQDN II* saw the CJEU sitting as a full Court. This case comment examines three potential interrelated reasons for the recourse to a full Court in *LQDN II,* contextualises the most essential aspects of the Court's ruling, and critically engages with each of the two Opinions issued by the Advocate General over the course of proceedings. It argues that the ramifications of the judgment in *LDQN II,* coupled with its sister judgment in *Bolzano,* issued on the same day, are likely to reach well beyond copyright to influence the future of criminal law enforcement in the EU more broadly, and ultimately the future of anonymity online.

1. Introduction

At first glance, it was not the hottest ECJ judgment last spring: 165 paragraphs of peer-to-peer file sharing protocols, mass copyright infringements and 'three strikes' warn-and-fine systems – less ominous criminal threat than long-standing nuisance, and arguably a largely private one at that.

Indeed, for criminal lawyers it was not even the hottest judgment handed down that day (30 April 2024), which also saw rulings on the monitoring of traffic and location data in cases of aggravated theft[1] and a coordinated law enforcement takedown of an entire encrypted mobile phone network[2] used inter alia[3] by organised criminals.

Yet Case C-470/21 *La Quadrature du Net* ('*LQDN II*'),[4] wherein the CJEU held that EU law does not preclude national law imposing the blanket[5] retention by electronic communications service providers of IP addresses for the subsequent use of the relevant public authorities in the fight against copyright infringements online – ie. offences that are usually not considered "serious" crime – was the only one of those three judgments to be decided by a full Court.

In Article 60(2) of the Court's Rules of Procedure one reads that a full

Article 15(1) of the e-Privacy Directive; Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights

* Corresponding author.
E-mail address: g.l.robinson@law.leidenuniv.nl.

[1] Case C-178/22 *Procura della Repubblica presso il Tribunale di Bolzano* ECLI:EU:C:2024:371 ('*Bolzano*').

[2] Case C-670/22 *M.N. (EncroChat)* ECLI:EU:C:2024:372.

[3] J.J. Oerlemans and D.A.G. van Toor, 'Legal Aspects of the EncroChat Operation: A Human Rights Perspective' (2022) 30 European Journal of Crime, Criminal Law and Criminal Justice, 309.

[4] Case C-470/21 *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* ECLI:EU:C:2024:370 ('LQDN II, judgment').

[5] As in: general and indiscriminate in terms of personal scope; covering all users.

https://doi.org/10.1016/j.clsr.2025.106178

Available online 8 August 2025

Court is reserved for cases of 'exceptional importance'.[6] Doubtless, around these proceedings there was and remains a degree of political pressure from France,[7] a few years after the dramatic fallout[8] from the seminal 2020 judgment in *LQDN I* (discussed further below),[9] and a few months before the arrest of the Telegram founder Pavel Durov[10] at Le Bourget airport in another strike against the perceived risk of rampant impunity online.

But what else about the sequel – in particular, from a legal perspective – might have warranted the extremely rare recourse to the *séance plénière?* Why, exactly, was this case deemed significant enough?

This case comment examines three potential interrelated reasons for the recourse to a full Court in *LQDN II*.

The first suggested reason is the opportunity presented by these proceedings to reconcile two strands of the Court's own case law, otherwise in tension – if not conflict. The second is a need to thoroughly examine or 'stress-test' a notion found at the heart of the Court's reasoning in this case, as it sits at the fulcrum of its stance on data retention for over a decade – the concern to ensure that data enabling the drawing of 'precise conclusions' about the private lives of individuals receive the strictest of proportionality tests – and to do so in an enforcement setting that is technologically complex. The third and last posited reason for recourse to a full Court in *LQDN II,* nominally a 'copyright case', comes down to its possible broader ramifications of the judgment for EU data retention law and the enforcement of the criminal law in our hyper-digital times. Along the way, the case comment contextualises the most essential aspects of the Court's ruling, and critically engages with each of the two Opinions issued by the Advocate General over the course of proceedings.

2. Reason #1 – The opportunity to reconcile CJEU case law on copyright and data retention

The first suggested reason is that in *LQDN II* the Court faced the confluence of two lines of its own case law (on copyright enforcement on the one hand, and on the pre-emptive retention of communications data for the purposes of combatting crime on the other) which are not only especially complex both legally and technologically, but also potentially incompatible. To see how, we'll need to first sketch the essential facts behind *LQDN II*.

2.1. I only have IPs pour vous… copyright enforcement (in France) and EU law

The proceedings in *LQDN II* revolved around the activities of Hadopi (the *Haute Autorité pour la Diffusion des Œuvres et la Protection des droits d'auteur sur Internet*), the French national agency tasked with encouraging and enforcing compliance with copyright laws on the internet. After proceedings began, Hadopi merged with the CSA (*Conseil supérieur de l'audiovisuel)* to form ARCOM (*Autorité de regulation de la communication audiovisuelle et numérique*), with the latter taking over the operation of the copyright enforcement mechanism known as the 'graduated response' (*réponse graduée*) in essentially unchanged form.

Enforcement setups like the French one under scrutiny in *LQDN II* have often been called 'three strikes' systems: in the case at hand, the first 'strike' consists of a recommendation/warning sent to the person whose internet connection has been used to infringe copyright online – for instance, sharing videos on a peer-to-peer file sharing protocol. If there is a repeat infringement within a year, the second strike consists of a warning that the conduct may constitute either the minor offence of gross negligence or the more serious offence of counterfeiting. After deliberation by Hadopi's (now ARCOM's) 'rights committee', a third strike may consist in a report sent to the public prosecutor's office, for the latter to pursue the case as either gross negligence (punishable by a maximum fine of 3000 euros) or counterfeiting (punishable by three years' imprisonment and a fine of 300,000 euros.

To operate this kind of system aiming to protect one kind of IP (intellectual property), public agencies like Hadopi need to be able to link online usernames with real-life individuals behind the usernames – or at least, as a first step, the real-life individual(s) behind the internet *connection.* This is where another kind of IP comes in: the internet protocol addresses from which files are shared, which can be gleaned directly from peer-to-peer sharing protocols using programmes designed for that very purpose.

That has long been done by rightsholders' associations or by private companies who never intend to exploit the IP themselves but merely pressure users (hence the moniker 'copyright trolls') into paying settlements in return for not progressing a claim. That practice has already been examined at length by the Court.[11] To cut another long story short: whilst the proper status of 'copyright trolls' under EU copyright law comes down to a case-by-case assessment by the national court, Member States may – but are not obliged to – establish a duty on private actors to retain IP addresses for the purposes of privately enforcing copyright breaches. So long as GDPR compliance is there, there is in principle nothing in EU law to oppose the activities of 'copyright trolls'.

In any case, and irrespective of their provenance, after suspect IP addresses have been delivered to a public agency such as Hadopi that agency still needs to work out who is behind them before it can start the enforcement process.

Bona fide personal and contact details (name, address, telephone number, email address) for those individuals will often be held by the suspected infringers' internet access provider (or, potentially, their VPN service provider) – but to make the link between the IP address scooped up online and the customer of the internet access provider, the latter will *also* need to have a record of the IP addresses assigned to those customers, either on a static (permanent) or dynamic basis (if the latter, further information such as timestamps will also be required to discern who used a given IP address at time of upload).

Without that information, there is simply no way for an internet access provider to match the suspect IP addresses to their customers. And this is precisely where, in *LQDN II,* French copyright enforcement ran up against the Court's body of data retention case law. For whilst it was already established in the latter that national law may, in principle and in full compliance with Charter rights, provide for the blanket retention by electronic communications service providers of *data relating to civil identity* for the purposes of combatting all crime (thus: including copyright offences), retention of *traffic data* – a data *category* that, at least for EU law, encompasses the IP address as a data *type* – was subject to a more stringent regime.

[6] *Consolidated version of the Rules of Procedure of the Court of Justice of 25 September 2012,* available at https://curia.europa.eu/jcms/upload/docs/application/pdf/2012-10/rp_en.pdf

[7] Xavier Groussot and Annegret Engel, 'Op-Ed: "The Devil is in the (Procedural) Details – The Court's Judgment in La Quadrature du Net", *EU Law Live*, 13 May 2024, available at https://eulawlive.com/op-ed-the-devil-is-in-the-procedural-details-the-courts-judgment-in-la-quadrature-du-net-by-xavier-groussot-and-annegret-engel/

[8] Jacques Ziller, 'The Conseil d'Etat refuses to follow the Pied Piper of Karlsruhe', *Verfassungsblog,* 24 April 2021, available at https://verfassungsblog.de/the-conseil-detat-refuses-to-follow-the-pied-piper-of-karlsruhe/

[9] Case C-511/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791 ('LQDN I, judgment').

[10] Damien Leloup and Benjamin Quénelle, 'Telegram CEO Pavel Durov arrested in France in world-first case', *Le Monde,* 25 August 2024, available at https://www.lemonde.fr/en/pixels/article/2024/08/25/telegram-ceo-pavel-durov-arrested-in-france-in-world-first-case_6721434_13.html

[11] Case C-597-19 *M.I.C.M.* ECLI:EU:C:2021:492.

2.2. Not just any old traffic data: the place of IP addresses within the data retention case law

In its judgment in *LQDN I*,[12] the Court effectively issued a compendium of its data retention case law up to that point, based around what Mitsilegas et al. call a 'hierarchy of security objectives'[13] to structure the contours of (potentially) Charter-compliant retention of communications data. In descending order of importance, those objectives are: safeguarding national security; combatting serious crime and preventing serious threats to public security; and combatting all crime and preventing non-serious threats to public security. The more intrusive the data category to be retained, the more important the public interest (security) objective constituting the reason for that retention (and the intended ultimate use of the retained data) will have to be to avoid censure on Charter grounds.

So it is that *content data* – as the most intrusive data category – may never be subject to a pre-emptive (or if one prefers, 'suspicionless') retention mandate, for any of the stated purposes, as to do so would violate the essence of the Charter rights at stake.[14] On the other end of the intrusiveness spectrum, *civil identity data* – corresponding closely, if imperfectly, to the traditional category of *subscriber data* – may be retained in general and indiscriminate fashion, to be accessed for any of the stated purposes (ie even for minor crimes).[15]

Somewhere between those two poles of acceptability sit traffic and location data, ever since the Court's groundbreaking 2014 judgment in *Digital Rights Ireland* in which it voiced very strong concerns about the profiling potential of metadata, information which, "taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained".[16] In the follow-up judgment in *Tele2*, the Court subsequently observed that communications metadata may provide a means "of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications".[17]

In *LQDN I,* the Court reaffirmed and developed its earlier case law in holding that, as data categories, and crucially subject to substantive and procedural safeguards that I will not detail here, traffic and location data may be pre-emptively retained for the purposes of combatting serious crime and preventing serious threats to public security on the condition that retention is 'targeted' (in terms of persons whose data are retained, or specified geographical zones, or otherwise), as opposed to 'general and indiscriminate' (all users). In the years since, only a handful of Member States have legislated or proposed national targeted metadata retention schemes, and the extent to which they risk turning the exception into the rule is contested.[18]

But our focus here is on IP addresses. Pre-*LQDN II,* where did they fit in? The first part of the answer is: as a discrete data *type* within the data *category* that is 'traffic data', because, just like other traffic data, their retention constitutes a serious interference with Charter rights insofar as they may be used to 'track an Internet user's complete clickstream and, therefore, his or her entire online activity'.[19] The second part of the answer, however, is that unlike other traffic data their retention need *not* be targeted – so long as only IP addresses assigned to the source of a communication are retained – since, unlike destination IP, 'those addresses do not, as such, disclose any information about third parties who were in contact with the person who made the communication'.[20] The source/destination distinction is sometimes elided, even in expert commentary, but it was subsequently clearly reaffirmed, for instance in *SpaceNet: source* IP may be generally and indiscriminately retained, but for the purposes of combatting *serious* crime only.[21]

This settlement, with IP addresses holding a kind of middle ground within the middle ground occupied by traffic data (together with location data), stood until *LQDN II.*

2.3. The first AG opinion: 'a certain tension' between private and public enforcement of offences 'committed online'

In his first Opinion in *LQDN II,* AG Szpunar summarised the situation as follows: '[t]he obligation to disclose personal data to private persons to enable them to bring civil proceedings for copyright infringements, which was made possible by the Court itself, is therefore simultaneously cancelled out by the effect of its own case-law on the retention of IP addresses by providers of electronic communications providers'.[22]

As mentioned earlier, the Court's data retention standards had been directly challenged by Member States on many previous occasions: always on the platform of a (more or less) distinct national regime, and always seeing Member States – one way or another – seeking a 'reconsideration' of the *effet utile* reasoning underpinning the jurisprudence from *Tele2* onward. The Court had even brushed aside a challenge based on national law whose existence had been required by EU law: in *VD and SR,* where the French government was unsuccessful in persuading it that the retention of communications data was a legally-stipulated condition for the effective fight against market abuse, seeing as the EU's own Market Abuse Regulation demands that competent authorities be able to require 'existing data traffic records held by a telecommunications operator'.[23] Ultimately, in that case the Court decided that 'existing' data referred to data 'if they happen to exist', as opposed to data that 'must (still) exist' – for example, through a mandatory data retention scheme.[24]

The very fact that, this time, a challenge to the well-established data retention case law had now come from another corner of the Court's own canon may already go some way toward explaining the recourse to a full Court in *LDQN II.* Add to that both the reasoning employed by the AG and the solution he proposed – in a nutshell, that under certain

[12] Previously discussed in this review in Xavier Tracol, 'The two judgments of the European Court of Justice in the four cases of *Privacy International, La Quadrature du Net and Others, French Data Network and Others* and *Ordre des Barreaux francophones et Germanophone and Others:* The Grand Chamber is trying hard to square the circle of data retention' (2021) 41 *Computer Law & Security Review* 105540.

[13] Valsamis Mitsilegas, Elspeth Guild, Elif Kuskonmaz and Niovi Vavoula, 'Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks' (2022) 1-2 European Law Journal 176, 181.

[14] Case C-293/12 *Digital Rights Ireland and Seitlinger and Others* ECLI:EU:C:2014:238, paras 38-39. See further Maja Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (2019) 20 *German Law Journal* 864.

[15] Case C-207/16 *Ministerio Fiscal* ECLI:EU:C:2018:788.

[16] *Digital Rights Ireland*, op cit, para 37.

[17] Case C-203/15 *Tele2 Sverige* ECLI:EU:C:2016:970, para 99.

[18] Gavin Robinson, 'Targeted Retention of Communications Metadata: Future-proofing the Fight Against Serious Crime in Europe?' (2023) 8(2) European Papers 713, 733.

[19] LDQN I, judgment, para 153.

[20] LQDN I, judgment, paras 152, 155.

[21] Case C-793/19 *SpaceNet* ECLI:EU:C:2022:702, paras 97-103.

[22] Opinion of Advocate General Szpunar in Case C-470/21 *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* ECLI:EU:C:2022:838, 27 October 2022 ('LQDN II, first Opinion'), para 76.

[23] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC [2014] OJ L173-1, Article 23(2)(h).

[24] Case C-339/20 *VD and SR* ECLI:EU:C:2022:703, para 77.

conditions source IP addresses should be retained and accessed *as if they were* civil identity data – and the stakes of the case become clearer.

Other paths were, conceivably, open to the AG. He might have confirmed the illegality of France's blanket retention of IP for less-than-serious criminal offences,[25] perhaps explaining the present 'tension' in the case law between public and private enforcement as emanating, at root, from the very settlement reached in the ePrivacy Directive in 2005 – a settlement of such import to fundamental rights that only the EU *legislature* could reconfigure it – either via the underlying regulatory framework (a new ePrivacy Regulation) or a fresh data retention law (more on that prospect below).

Instead, in a sort of boomerang of the *effet utile* reasoning at the heart of the Court's stance since *Tele2,* in his first Opinion the AG reached for the 'utility argument': where IP addresses are the *only means* of investigating criminal offences committed online, this indispensability ought to justify a 'readjustment' of the case law to accommodate the retention of and access to source IP even for non-serious crime.[26] In doing so, the AG picked up a thread left by the Court in its ruling in *LQDN I,* where the Court reasoned that since source IP might be the only means to combat CSA and terrorist offences, the balancing of interests dictates that blanket retention should be permitted for the purpose of combatting serious crimes. Here, essentially, that same argument is used to propose an extension of blanket retention of source IP to the fight against some non-serious crimes.

Just where might such a 'readjustment' lead? Could potentially any crime, however minor, 'committed online', and whose enforcement can be said to depend on law enforcement access to IP addresses fall into scope? The AG himself used the example of online defamation – a startling gear change from the Court's earlier evocations of CSAM and terrorism.

3. Reason #2 – A need to stress-test the 'precise conclusions' threshold

With all of the above in mind, it may seem less surprising that the procedure was then exceptionally reopened, with parties invited to deliberate on a long list of questions.[27] One set of questions, designed to catch all aspects of the dispute and possible solutions thereto, was put to the full ensemble of parties summoned (back) to Luxembourg, with another set on the exact inner workings of the Hadopi enforcement system put to the French government. Interestingly, the European Data Protection Supervisor and the EU's cybersecurity agency ENISA were also invited to comment, at fresh hearings, on the written answers provided by parties on a variety of matters including whether it is technically possible to access other traffic data and location data with retained IP in hand, and possible alternatives to prior independent (judicial) review of access to retained IP – in light of the sheer numbers of discrete copyright infringements that are committed daily online.

A second Opinion from the AG followed in September 2023, just under a year after the first.[28] At 90 paragraphs, it was nearly as lengthy as the first, which ran to 111 paragraphs. There are several subtle differences between the AG's two Opinions, but here I briefly tackle only two central developments: the gravity of the interference with Charter rights constituted by blanket retention of source IP, and the AG's expanded discussion of the reasoning behind and envisaged outer limits of the 'utility argument', as I termed it above.

In contrast to the first Opinion, where retention *and* access to blanket-retained source IP were viewed as serious interferences with Charter rights – justified, all the same, by the indispensability of those data to the fight against certain offences committed online – in the second Opinion that interference is no longer serious: or, to use the AG's vocabulary, 'the seriousness of the interference' should be 'nuanced'.[29] To get to his final view that that interference is 'of limited seriousness',[30] the AG harnesses several features of the Hadopi enforcement scheme one can safely assume were lengthily discussed at the second ECJ hearing.

Most significantly, Hadopi agents only handle the civil identity data of suspected persons, associated IP, and an extract from the file uploaded in breach of copyright. The AG is confident that this triangle of elements 'do[es] not result in very precise conclusions about that person's private life being drawn' ;[31] moreover, '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' that 'reveal much less information about the person's private life'.[32] Dynamic IP addresses also make a first appearance, in support of the same determination: these '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', precluding any exhaustive tracking.[33]

Together with this clarification of the AG's stance with regard to the '(very) precise conclusions' yardstick both in terms of its general application and the specific Hadopi scenario, we find an intriguing rumination on the 'utility argument' already noted above – in particular, an emphasis on the *identification* of (sometimes 'suspected', sometimes confirmed) wrongdoers, as distinct from criminal *investigation*. For the AG, "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'.[34] Where it *does* depend on a single means of investigation, in this case source IP, the alternative to ensuring its availability through retention mandates is would be to accept 'that a whole range of criminal offences may evade prosecution entirely'.[35]

3.1. The ECJ ruling: retention of IP to fight non-serious crimes (… committed online?)

Half a year further on, and the ECJ ruling that arrived was mostly in line with the AG's second Opinion. Both, overall, carve out more space for the general and indiscriminate retention of IP addresses to be accessed and used in the fight against crime, relying on a similar 'direction' of reasoning to do so. However, some of the Court's emphasis is markedly different, it adds several important new considerations of its own, and the endpoint is also technologically distinct, in that its verdict ostensibly refers to *all* IP addresses rather than merely source IP – although, curiously, no direct explanation for this difference is given.

Much more attention is paid in the judgment to the notion of (very) precise conclusions regarding the private lives of individuals, which permeate its deliberations as regards both retention of IP addresses and access thereto. The phrase 'precise conclusions about private life' is

[25] Chloé Berthélémy, Jesper Lund and Bastien Le Querrec, 'A complete U-turn in jurisprudence: HADOPI and the future of the CJEU's authority', *European Law Blog,* 4 December 2023, available at https://www.europeanlawblog.eu/pub/a-complete-u-turn-in-jurisprudence-hadopi-and-the-future-of-the-cjeus-authority/release/1

[26] LQDN II, first Opinion, paras 82-83.

[27] Order of the Court in Case C-470/21 *La Quadrature du Net and Others () and lutte contre la contrefaçon)*, 23 March 2023, ECLI:EU:C:2023:256.

[28] Opinion of Advocate General Szpunar in Case C-470/21 *La Quadrature du Net and Others () and lutte contre la contrefaçon),* ECLI:EU:C:2023:711, 28 September 2023 ('LQDN II, second Opinion').

[29] LQDN II, second Opinion, para 54.

[30] LQDN II, second Opinion, para 63.

[31] LQDN II, second Opinion, para 50.

[32] LQDN II, second Opinion, para 53.

[33] LQDN II, second Opinion, para 51.

[34] LQDN II, second Opinion, para 60 (citing *LQDN I, GD* and *SpaceNet*).

[35] LQDN II, second Opinion, para 62.

repeated no less than 22 times in the 113 paragraphs that form the Court's consideration of the questions referred. Both the mention-count (against only 6 in the AG's second Opinion) and the 'in principle' carefully inserted into the cited sentence would tend to suggest that technical possibilities to do so may well exist – and indeed, a careful reading of the AG Opinions does not dispel this concern.

Largely for this reason, whilst one reads in the judgment that as Hadopi does not have access to 'a set of traffic or location data' […] it cannot, in principle, draw precise conclusions about the private life of the persons concerned',[36] the Court is doubly clear that national legislation must both limit the use of retained IP to identification of the person to whom a particular IP address was assigned and preclude 'any use that allows the surveillance, by means of one or more of those addresses, of that person's online activities'.[37] A kind of legal fiction introduced by the AG is thereby confirmed by the Court: 'access to that address for that sole purpose concerns that address *as data relating to civil identity rather than as traffic data*'.[38] All being well (from an enforcement perspective), IP addresses effectively jump out of the box marked 'traffic data' and into the box marked 'civil identity data'.

At the national level, interested readers of this passage of the judgment will likely have included the Belgian legislators, practitioners and commentators who have tussled over the inclusion of IP addresses within the baseline category of 'identification data' in the latest data retention law in that country.[39] This interpretation from the Court in *LQDN II* certainly tends toward confirming the EU-legality of such an approach, which would otherwise most likely have run afoul of the *LQDN I* line of jurisprudence.

If the reader can forgive the repetition: if IP is to be used to combat crime, it must first be retained for that purpose. Here too, in the spirit of precluding the drawing of 'precise conclusions', the Court opens a new dimension in its case law by stipulating that any IP addresses retained must be retained separately from other data categories (such as civil identity data, location data and other traffic data) by the *service provider*. Such separation must be "genuinely watertight".[40] This novel extension of the Court's reach 'upstream' into the regulation of retention operations carried out on the *private* actor's side generates new questions. Whilst it is deemed essential to preclude the drawing of precise conclusions, it is never quite made clear who might be drawing said conclusions. The service providers themselves? The (public) investigators with the power to eventually obtain access to retained data? A mix of both? In this respect, the Court might have been more explicit on the relative risks of a chilling effect attracted by retention by private actors on the one hand, and access for public enforcers on the other.

Lastly for this section, and as noted above, the Court follows its AG in validating the retention (so long as all its conditions are met) of IP addresses for the purposes of combatting copyright infringements. Like the AG, it too provides guidance on the potential scope of its reasoning beyond copyright. But here, the two also diverge insofar as the Court makes no mention of the AG's key 'utility argument' in its answer to the referring court. Indeed, whereas the AG included the 'indispensability' of IP addresses as a condition within his proposed legal test for Charter-compliant retention of source IP, the Court, more straightforwardly, greenlights the retention of all IP (so long as all its other conditions are met) for the purpose of fighting non-serious criminal offences, before explaining that such retention is adjudged to be 'strictly necessary for the attainment of the objective pursued'.[41]

Which crimes does the Court see as a 'real risk of systemic impunity', should IP addresses escape blanket retention measures? '[N]ot only […] criminal offences infringing copyright or related rights, but also […] other types of criminal offences committed online *or the commission or preparation of which is facilitated by the specific characteristics of the internet*'.[42] This strikingly open-ended formulation is only slightly reined in by the ensuing sentence: '[t]he existence of such a risk constitutes *a relevant factor* for the purposes of assessing' proportionality of retention schemes.[43] I return to the question of non-serious and serious crime below, when I discuss the crucial judgment issued on the same day as *LQDN II* (and mentioned at the outset of this case comment) in *Bolzano*. First, however, I will complete the overview of the Court's determinations in *LQDN II* by addressing its position on *access* to retained IP addresses.

3.2. The ECJ ruling: access to retained IP, prior review and data protection for law enforcement

Access to retained IP is where the Court departs the most from its AG's recommendations – and it does so in two main aspects. First, it provides tailored guidance to the French court on the kind of prior review that is required under the specific circumstances, whereas the AG had seen no need for prior review at all, either in the Hadopi scenario or *any* duly-justified access to IP for 'online' criminal offences. And second, it effectively conditions its acceptance of IP retention for non-serious crime on the existence – and verification – of data protection standards in law enforcement, with explicit reference to the LED (in his two Opinions, the AG had only mentioned that instrument in passing).[44]

For the Court, 'precise conclusions' are also the *fil rouge* when it comes to prior review. The judgment is careful to insist that the 'precise conclusions' test must be applied holistically to the workings of any national enforcement scheme, rather than tunnelling in on access to retained IP per se. Subject to confirmation by the referring court, the ECJ gathered that alongside retained IP addresses, Hadopi *also* receives – from rightsholders organisations – a glimpse of the content being exchanged on P2P services by way a 'chunk' (or extract) and file names.[45] Might combining that information with civil identity data, in practice, enable Hadopi agents to draw 'precise conclusions' about the private lives of users, 'including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health'?[46]

The Court's answer (mirroring that of its AG) is: possibly so, but only in 'atypical situations' – for instance, where many files have been uploaded[47] – and several features of the Hadopi setup (sworn officials; access exclusively to identify a wrongdoer; obligation of confidentiality) swiftly line up to cement its determination of the non-seriousness – in principle – of the interference with Charter rights. Interestingly, however, the residual risk of serious interferences later reemerges when the Court deliberates on the suitability of prior review under the circumstances. Traffic data requires such a review, but civil identity does not. What of 'traffic data retained and accessed *as* civil identity data'?

[36] LQDN II, judgment, para 99.
[37] LQDN II, judgment, para 101.
[38] LQDN II, judgment, para 101, emphasis added.
[39] For an expert overview see Vanessa Franssen and Catherine van de Heyning, 'Belgium's New Data Retention Legislation: Third Time Lucky, or Three Strikes and You're Out?' in Eleni Kosta and Irene Kamara (eds), *Data Retention in Europe and Beyond: Law and Policy in the Aftermath of an Invalidated Directive* (OUP, 2025), 251.
[40] LQDN II, judgment, para 84.
[41] LQDN II, judgment, para 118.
[42] LQDN II, judgment, para 119, emphasis added.
[43] LQDN II, judgment, para 119, emphasis added.
[44] 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 [2016] OJ L119/89 ('LED').
[45] LQDN II, judgment, para 109.
[46] LQDN II, judgment, para 110.
[47] LQDN II, judgment, para 111.

After reviewing its relevant jurisprudence (*Ministerio Fiscal* and *Prokuratuur*[48] alongside *LQDN I*), the Court then runs a more privacy-protective line of reasoning: since '[i]t cannot be ruled out that, taken together and as the graduated response administrative procedure unfolds, the data thus provided in the various stages of that procedure may reveal concordant and potentially sensitive information about aspects of the private life of the person concerned thus making it possible to establish a profile of that person',[49] increasingly the *likelihood* of an increase in the intensity of the infringement of the right to respect for private life as the process goes on,[50] there must be no automatic linking of the two more anodyne data types (civil identity data and IP) with potentially sensitive snippets of the uploaded content.[51]

Whenever Hadopi agents wish to 'link' those three sources with a view to making a referral to the public prosecutor (thus, when shifting from the second stage to the third stage of the graduated response mechanism), that is when they are required to apply for prior review by a court or an independent administrative authority. It falls to the latter (whether court or other authority) to assess whether this 'linking' would allow precise conclusions to be drawn about the private life of the suspected person. If it would, there are two possible outcomes. Where the suspicion is of counterfeiting – which, the Court underlines, it is within the purview of a Member State to consider 'serious' – it *should* authorise access.[52] If the suspicion is of gross negligence, 'within the scope of criminal offences in general', however, access *must* be refused.[53]

What is one to make of the welding of such prescriptive guidance onto a body of case law that, as the AG had put it in his second Opinion, already 'bears all the hallmarks of a somewhat case-by-case approach'?[54] That the 'linking' of civil identity and IP to 'chunks' of content and filenames has been isolated as *the* moment when the risk of precise conclusions is certainly workable, even if it has already been challenged as arbitrary by Jongsma.[55] Most significantly, it immediately raises the question of how it could affect diverse national schemes spanning enforcement actions taken against a whole swathe of non-serious criminal offences. To pick only two of the open ends available (and also both noted by Jongsma): what *kind* of precise conclusions should tip the balance for review instances, and – if suspicions of serious crime *should* suffice to secure access – does this present an incentive to national legislators to consider more and more online offences as serious?

For the second time in this case comment, the trail leads to a dedicated discussion of the notion of 'serious crime' that was most recently addressed by the Court in *Bolzano* – even if, surprisingly, no cross-reference to that judgment is to be found in *LQDN I*. Before we get there, however, a word on the second of the judgment's two main novelties vis-à-vis the AG Opinions: a renewed emphasis on data protection for law enforcement.

In this regard, and in somewhat inverse fashion to the granular answer on prior review just discussed, the guidance issued by the Court is clearly for a broader audience than France alone. French law was indeed already unequivocal that Hadopi (now ARCOM) is considered a 'competent authority' in the French implementation of the LED, triggering application of the suite of law enforcement-specific informational norms to be found in that Directive. The Court's intervention on this matter is significant in the context of the data retention case law as a whole, where the regulation of retention has been shifting toward regulation of access,[56] with *LQDN II* now taking this further into regulation of the broader *use* of retained data, from a reminder to Member States that substantive and procedural safeguards include concerned persons' rights of access, rectification and erasure of personal data processed by the enforcement body,[57] to national courts who are (also) tasked with ascertaining whether national implementing laws measure up.[58] The message for onlookers across the Member States is thus clear: for any enforcement entity to access retained IP in the pursuit of perpetrators of non-serious offences, the standards in the LED must be a functioning reality.

4. Reason #3 – The wider (criminal) policy ramifications of the ruling

As noted above, given the central importance of the notion of serious crime to both cases it is puzzling that the Court makes no mention of *Bolzano* in its judgment in *LQDN II,* if only to help interested readers navigate the ties between the rulings, issued on the same day (*Bolzano,* for its part, refers to *LQDN II* on three occasions). Without going into unnecessary detail on the facts or reasoning in *Bolzano,* how do the two judgments interlock?

4.1. The sister judgment in Bolzano and the outer limits of 'serious' crime

In short, the judgment in *Bolzano* appears to aim at dampening any Member State inclinations to stretch the notion of 'serious crime' beyond tolerable limits – whether to open the door for the use of traffic and location data caught under new 'targeted' retention schemes (that I will not unpack here) in the pursuit of otherwise minor offences, or to dispense with the tighter review standards for blanket-retained IP.

Recall that, as of *LQDN II,* national law may in principle mandate the blanket retention of IP addresses to be used in combatting crime – both serious and non-serious offences. However, not only is prior review required wherever 'precise conclusions' can be drawn about the private life of the suspected person, but there is also the plain instruction to the review authority that access *must* be refused if the offence is non-serious. Granted, the need for a prior review in the first place only exists when said 'precise conclusions' can be drawn (and IP addresses alone will not enable this), but some degree of temptation for national legislators to 'scale up' offences from non-serious to serious would seem inevitable.

A comparable development in national law had in fact already triggered the proceedings in *Bolzano*: after the Italian Supreme Court of Cassation held in 2021 that the CJEU's case law did not have the characteristics required for it to be applied directly by the national courts, the Italian legislature amended the relevant decree in order to classify as serious offences, for which telephone records may be obtained, offences which are punishable by law by a maximum term of imprisonment 'of at least three years'.[59] According to the referring court, that test would catch 'offences which cause only a limited social disturbance and which are punishable only on foot of a complaint by a private party, in particular low-value thefts such as mobile phone or

[48] Case C-746/18 *Prokuratuur* ECLI:EU:C:2021:152.
[49] LQDN II, judgment, para 139.
[50] LQDN II, judgment, para 140.
[51] LQDN II, judgment, para 142. As an aside, the Court also made light work of the referring court's request for guidance on the permissible contours of automated review, since when it comes to intellectual property infringements, the numbers can run into the millions. Can review be automated? The query is handled in 4 laconic paragraphs, encapsulated in turn by the following 10 words: 'a prior review may in no case be entirely automated'; para 148.
[52] LQDN II, judgment, para 146.
[53] LQDN II, judgment, para 145.
[54] LQDN II, second Opinion, para 86.
[55] Daniël Jongsma, 'The thorny issue of IP address retention and online copyright infringement: The Full Court shows the way in *La Quadrature du Net and Others*' 61(6) Common Market Law Review 1607. The author contends, moreover, that also in terms of *private* copyright enforcement the judgment 'probably raises more questions than it solves'; p. 1626.
[56] Eleni Kosta, 'The Evolution of the CJEU Case Law on Data Retention: Towards the Regulation of Access' in Kosta and Kamara (eds), op cit, 13.
[57] LQDN II, judgment, para 161.
[58] LQDN II, judgment, para 163.
[59] *Bolzano,* judgment, para 20 and sources cited therein.

bicycle theft'.[60]

The Court's response in its judgment in *Bolzano* was to underline that Member States 'cannot distort the concept of 'serious offence' and, by extension, that of 'serious crime', by including within it […] offences which are manifestly not serious offences, in the light of the societal conditions prevailing in the Member State concerned, even though the legislature of that Member State has provided for such offences to be punishable by a maximum term of imprisonment of three years'.[61]

The Court went on to underline that national courts 'must be able to exclude such access where it is sought in the context of proceedings for an offence which is manifestly not a serious offence',[62] raising the intriguing prospect of national courts systematically vetting individual instances of access to data in the concrete criminal proceedings, even where the offence qualifies as 'serious' by dint of both the maximum punishment it can attract *and* – in a manner reminiscent of the *Engel* jurisprudence at the European Court of Human Rights – its formal classification on the criminal law books.

4.2. Conclusion: The future of communications data retention in the EU

Four years on from *LQDN I,* where the Court accepted in principle (i) the general and indiscriminate retention of traffic and location data for the paramount purpose of safeguarding national security,[63] (ii) the targeted retention of those same data categories to fight serious crime and serious threats to public safety, (iii) the blanket retention of civil identity data for the combatting of any crime, and (iv) the blanket retention of source IP for serious crime, the (qualified) greenlighting of blanket retention of IP addresses to combat non-serious crime in *LQDN II* represents, for better or for worse, a further step in the loosening of EU law's grip on national data retention regimes – at least, that is, until a fresh Union-wide retention mandate can be agreed.

On the one hand, it opens new possibilities – well beyond the realm of copyright – for national initiatives to tip the balance toward the informational demands of law enforcement and away from a protective approach to Charter rights to respect for private and family life, to the protection of personal data, and to the freedom of expression and information online. On the other hand, however, there is the eminently arguable narrowness of the precedent: the many factual specificities of this complex case, together with the manifold qualifications and conditions issued by the Court in *LQDN II,* together with *Bolzano,* mean that the judgment defies any easy placement between two poles marked 'privacy' and 'security'.[64]

It remains to be seen whether this more accommodating approach from the Court might take the wind from the sails of efforts toward a new Union-wide data retention law or, on the contrary, contribute to ushering one in. There are certainly ongoing efforts to devise fresh legislation to reboot EU data retention (a project that has never, in truth, been too far from the policy table) – see for instance the November 2024 concluding report of the high-level expert group on access to data for effective criminal enforcement.[65] The report describes how 'the HLG experts discussed the need to design access rules which differ depending on e.g. the type and seriousness of the crime, the degree of threat posed to the victims by the offence, the purpose of access and the authorities competent to access the data'.[66] This follows in the slipstream of *LQDN II,* where the Court's earlier focus equating purpose of retention (and access) squarely to 'seriousness of crime' began to morph into a more holistic consideration of the goals of discrete enforcement arrangements (in this case, copyright enforcement) and of individual instances of access to *identify* a wrongdoer (in this case, a copyright infringer) whose responsibility is already more or less incontrovertible. It also dovetails with the new e-Evidence Regulation,[67] whose central measure – the European Production Order – requires a lighter regime for subscriber data and 'data requested for the sole purpose of identifying the user'.[68]

As international negotiations and EU policy-making continue to simmer away in the background, the impact of *LQDN II* over the longer term will likely boil down to three interrelated questions: the application (and workability) in practice of the 'precise conclusions' test; where exactly diverse national systems draw the line around the notion of serious crime; and which *non*-serious crimes are deemed to have an 'online' dimension that suffices to tip the proportionality scales toward blanket retention of IP addresses. It remains to be seen whether national legislators as well as national courts are inclined to use their new (or newly-reiterated) duties in a 'meaningful dialogue' on data retention with the ECJ,[69] lest this judgment's purportedly 'necessary and limited development'[70] of the case law hasten the death by a thousand cuts of the principle on which it has always rested: that retention of electronic communications must be an exception, with confidentiality remaining the rule.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

[60] *Bolzano,* judgment, para 21.

[61] *Bolzano*, judgment, para 50. See in detail Francesca Palmiotto, 'Criminal investigations, access to data and fundamental rights: The role of judicial review after *Procura'* 61(6) Common Market Law Review 1633.

[62] *Bolzano*, judgment, para 62.

[63] For a limited period of time, as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat to national security which is shown to be genuine and present or foreseeable. Verification that one of those situations exists must, furthermore, be entrusted to a court or an independent administrative body whose decision is binding, and that review must also encompass a check on the observation of further conditions and safeguards: instructions given to private parties to preventively retain the data of all users must be limited in time to what is strictly necessary (renewals are possible but cannot exceed a foreseeable period of time), and personal data must be effectively protected against the risk of abuse; LQDN I, judgment, paras 137-139.

[64] For a variety of perspectives on the *LQDN II* judgment, see further Erik Tuchfeld, Isabella Risini and Jakob Gašperin (eds), *Eyes everywhere: Surveillance and Data Retention under the EU Charter* (Verfassungsbooks, 2025).

[65] Discussed (with link to the HLG report) in Thomas Wahl, 'Spotlight: High Level Group Recommendations on Law Enforcement Data Access' (2024) 2024/4 *eucrim* 270-271. Available at https://eucrim.eu/media/issue/pdf/eucrim_issue_2024-04.pdf. See also most recently European Commission, 'Impact assessment on retention of data by service providers for criminal proceedings' (21 May 2025), available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14680-Impact-assessment-on-retention-of-data-by-service-providers-for-criminal-proceedings-_en

[66] HLG report, ibid, p. 35.

[67] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L191/118 ('e-Evidence Regulation').

[68] e-Evidence Regulation, Article 4(1), Recitals 36, 37 and 40. Indeed, the absence of an EU-level retention mandate is not infrequently held out as the biggest obstacle to the success of the e-Evidence package – and it may even be a main reason why, close to 2 years on from that package becoming law, and over 7 years since the CLOUD Act was passed, there is still no EU-US agreement on reciprocal direct cooperation for electronic evidence; see further Katalin Ligeti and Gavin Robinson, 'Sword, Shield and Cloud: Toward a European System of Public-Private Orders for Electronic Evidence in Criminal Matters?' in Valsamis Mitsilegas and Niovi Vavoula (eds), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Hart 2021), 27, 65-69.

[69] As the AG put it in his second Opinion; endnote 38.

[70] LQDN II, second Opinion, para 78.