CJEU: Data Retention Allowed in Exceptional 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
2020, Vol. 15(3) eucrim pp 184 – 186
ISSN: 1862-6947
https://eucrim.eu

On 6 October 2020, the Grand Chamber of the CJEU delivered its judgments on data retention concerning the British, French, and Belgian rules (Case C-623/17 (*Privacy International*), and Joined Cases C-511/18 (*La Quadrature du Net and Others*), C-512/18 (*French Data Network and Others*) and C-520/18 (*Ordre des barreaux francophones et germanophone and Others*)). The cases were referred to the CJEU following several CJEU judgments in recent years (in particular the 2016 judgment in *Tele2 Sverige and Watson and Others*) which precluded national legislation on the retention of and access to personal data in the field of electronic communications. The referring courts raised doubts as to whether the case law deprives Member States of an instrument considered necessary to safeguard national security and combat crime. For detailed information on the cases at issue and the opinion of the Advocate General à eucrim 1/2020, 22-23. The CJEU addressed the following questions:

Is the e-Privacy Directive applicable?

In its rulings, the Grand Chamber first counters arguments that Directive 2002/58/EC (the Directive on privacy and electronic communications, commonly referred to as the "e-privacy Directive") is not applicable in the present cases since the Directive excludes "activities concerning public security, defence and State security" from its scope (Art. 1(3) and the legislations at issue concern national security that falls outside the scope of EU law (Art. 4(2) TEU). The CJEU points out that the legislative data retention measures regulate data processing by private service providers and not "activities characteristic to the State", for which the Directive is exempted as referred to in Art. 1(3). Reference to Art. 4(2) TEU also cannot invalidate this conclusion, since the mere fact that a national measure has been taken for the purpose of national security cannot render EU law inapplicable and exempt Member States from their obligations to comply with that law.

Which forms of traffic and location data retention are precluded by Union law?

The referring courts asked whether Art. 15(1) of Directive 2002/58 precludes national legislation which imposes on providers of electronic communication services an obligation to retain traffic and location data for purposes of national and public security and combating crime. Art. 15(1) of Directive 2002/58 allows Member States to introduce exceptions to the principal obligation, laid down in Art. 5(1) of that Directive, to ensure the confidentiality of personal data (and to the corresponding obligations, referred to, *inter alia*, in Arts. 6 and 9 of that Directive), "when such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised

use of the electronic communication system." To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on one of those grounds.

The judges in Luxembourg principally upheld previous case law – the prohibition of "general and indiscriminate" data retention. This would also apply to cases in which telecommunication providers transfer data to security and intelligence agencies for the purpose of safeguarding national security as is the case for the British rules.

The same holds true for data retention as a preventive measure, which was specific to the French and Belgian legislation. These obligations to forward and retain traffic and location data in a general and indiscriminate way constitute particularly serious interferences with the fundamental rights guaranteed by the CFR, where there is no link between the conduct of the persons whose data is affected and the objective pursued by the legislation at issue. By further developing its case law in *Tele2 Sverige/Watson* and clarifying the interpretation of Art. 15 of Directive 2002/58, however, the CJEU allows several exceptions:

- General and indiscriminate retention of traffic and location data is allowed "in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable." Then, the following additional conditions must be fulfilled:
    - The decision imposing such an order is subject to effective review, either by a court or by an independent administrative body whose decision is binding;
    - The review verifies that one of the described situations exists and that the conditions and safeguards, which must be laid down, are observed;
    - The order is given only for a period limited in time to what is strictly necessary (there may be the possibility for extension, however, if the threat persists).
- Legislation can also provide for targeted retention of traffic and location data to combat serious crime and prevent serious threats. It is then required that this targeted retention is:
    - limited on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion;
    - limited to a period of time which is strictly necessary (but which can be extended).
- General and indiscriminate data retention of IP addresses assigned to the source of an Internet connection may be allowed in order to combat crime and safeguard public security, provided the retention is limited to a period of time which is strictly necessary.
- General and indiscriminate data retention relating to the civil identity of users of electronic communication systems is also allowed, whereby the Member States are not required to limit the retention period.
- Legislative measures can also allow recourse to an order for the expedited retention of data in the possession of service providers, provided that:
    - The purpose is to combat serious crime and, *a fortiori*, to safeguard national security;
    - The retention obligation relates only to traffic and location data that may shed light on serious criminal offences or acts adversely affecting national security;
    - The order is subject to effective judicial review;
    - The retention is undertaken for a specific period of time.

As cross-cutting requirements for all exceptions, the legislative measures must provide clear and precise substantive and procedural rules as well as effective safeguards against the risks of abuse.

Does Union law preclude the obligations for providers to implement measures allowing the automated analysis and real-time collection of traffic and location data?

The CJEU ruled that Art. 15(1) of Directive 2002/58, read in the light of Arts. 7, 8, 11, and 52(1) CFR, does not preclude national rules that require providers to take recourse, first, to the automated analysis and real-time collection of traffic and location data and, second, to the real-time collection of technical data concerning the location of the terminal equipment used. However, also here, several additional requirements must be observed by the national legislator:

As regards *automated analysis tools*:

- They must be limited to situations, in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable;
- Recourse to such analysis is subject to an effective review (either by a court or by an independent administrative body whose decision is binding);
- The aim of that review is to verify that a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed.

As regards the *real-time collection* of data:

- Recourse is limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities;
- A prior review is carried out (either by a court or by an independent administrative body whose decision is binding);
- The review ensures that such real-time collection is authorised only within the limits of what is strictly necessary;
- In cases of duly justified urgency, the review takes place within a short time.

May a national court limit the temporal effects of a declaration of illegality if the national legislation is held incompatible with Union law?

This question was specific to the Belgian situation. Although Belgian law empowers Belgian courts to suspend the temporal effects of illegality – with a view to, *inter alia*, safeguarding national security and combating crime – the CJEU observes that this would undermine the primacy and uniform application of EU law. Hence, the answer to the question was “no”. The CJEU argues that maintaining the effects of national legislation would mean that the legislation would continue to impose obligations on service providers that are contrary to EU law and which seriously interfere with the fundamental rights of the persons whose data has been retained.

The judges in Luxembourg noted, however, that the question implies whether EU law precludes, in criminal proceedings, the use of information and evidence obtained as a result of a data retention regime in breach of Union law. In order to give a useful answer to the referring court, they call to mind that, as EU law currently stands, it is, in principle, for the national law alone to determine rules on the admissibility and assessment of such evidence in criminal proceedings. Nonetheless, national evidence rules are not purely exempted from Union law, because Member States are obliged to respect the Union principles of equivalence and effectiveness. In this context, the CJEU specifies: “[T]he principle of effectiveness requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact.”

Put in focus:

The CJEU has updated its data retention saga. It involved the following judgments:

- Case C-301/06 (*Ireland v EP/Council* à eucrim 1-2/2009, 2-3), backing the choice of legal basis of the EU Data Retention Directive 2006/24/EC as a first pillar instrument (cf eucrim);
- Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland, and Seitlinger and Others* à eucrim 1/2014, 12[T2]), declaring the EU's Data Retention Directive 2006/24 invalid on the ground that the interference into fundamental rights, which resulted from the general obligation to retain traffic and location data, was not limited to what was strictly necessary;
- Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige, and Watson and Others* à eucrim 4/2016, 164), prohibiting Member States from maintaining national data retention regimes if they entail a general and indiscriminate retention of data;
- Case C-207/16 (*Ministerio Fiscal* = eucrim 3/2018, 155-157), backing Spanish legislation that provides public authorities' access to data relating to the civil identity of users of means of electronic communication for the purpose of investigating criminal offences.

The two judgments of 6 October 2020 further refine the CJEU's approach to data retention. By detailing exceptions from a general and indiscriminate (national) data retention regime, the CJEU has drafted a possible model for data retention at both the European and national levels. On the one hand, the CJEU accommodates law enforcement, although the rather complicated model of exceptional cases allowing data retention for preventive purposes a kind of mirage. On the other hand, it remains to be seen whether this concept can be implemented by the legislators and whether it proves practicable for law enforcement authorities. The judgments will certainly also have an impact on other pending references for preliminary rulings, such as that of the German Federal Administrative Court (Bundesverwaltungsgericht) in Cases C-793/19 and 794/19, which seeks guidance on the compatibility of the German rules on data retention (à eucrim 3/2019, 176). Nonetheless, the outcome of these references still remains unclear. In addition, the judgments will have repercussions on the current discussion at the EU level about re-introducing harmonised EU rules on data retention for law enforcement purposes (for the discussion and the pushes from the Council à eucrim 4/2019, 236 and eucrim 2/2019, 106)

Reactions:

The media and experts commented on the judgments differently.

Privacy International, who brought the case concerning the UK, praised that the judgment reinforces the rule of law in the EU. In a press release that responds to the judgment, it mainly stresses three important issues:

- "EU law applies every time a national government forces telecommunications providers to process data, including when it is done for the purposes of national security.
- EU law sets out privacy safeguards regarding the collection and retention of data by national governments, which countries such as the UK, France and Belgium must follow.
- The cases will now return to each individual country's courts for implementation of the judgment."

La Quadrature du Net who brought the French case said: A first reading of the judgment suggests that it was a "victorious defeat". It concluded: "French law thus ends up in flagrant contradiction with the decision of the CJEU: the principle of bulk metadata retention is refused by the Court while it is the principle in France."

Statewatch commented: "In summary, it might be said that the state's surveillance menu is still rather extensive - but the buffet has been discontinued."

The Irish Independent draws a connection between the data retention judgment and the CJEU's recent ruling in *Schrems II* (eucrim 2/2020, 98-99) and believes that "the judgment moves the EU further away from coun-

tries such as the US and China, which integrate mass surveillance into their domestic security arrangements."

Euractiv points to ramifications of the judgment for the UK after Brexit since it might hinder the Commission from approving an adequacy decision that would enable data exchanges between EU and UK companies after the UK finally leaves the bloc at the end of this year.

Natasha Lomas wrote on TechCrunch that "a battle of definitions could be looming," although the CJEU made clear that bulk powers (as conferred to UK agencies) must be the exception, not the statutory rule.

Data protection expert *Juraj Sajfert* considers on European Law Blog that in particular the ruling in *La Quadrature du Net and Others* is a complex victory for the law enforcement community and a major step backwards in the Court's data *retention* jurisprudence. He analyses in detail the wins for both the privacy/data protection campaigners on the one hand, and the law enforcement community on the other hand.

The German IT news portal "heise.de" collected opinions from data protectionists and politicians. Data protectionists complain that the CJEU allowed exceptions to the previous ban on general and indiscriminate logging of user tracks for the first time. The portal cited Hamburg data protection supervisor *Johannes Caspar*, saying: "The CJEU has brought the 'old zombie' back to life." MEP *Patrick Breyer* fears that "the now permitted data retention of IP addresses makes it possible to 'screen' the private Internet use of normal citizens for months and make it transparent."

Sabine Leutheusser-Schnarrenberger, former Federal Minister of Justice, commented on Verfassungsblog: "The European Court of Justice has stood firm: There can be no mass surveillance of EU citizens without cause." She added that the exceptions made by the CJEU cannot serve as a basis for a blanket reintroduction of data retention as in the current framework. *Leutheusser-Schnarrenberger* also pointed to scientific studies that question the added value of the mass storage of telecommunication traffic, and location data for the prevention and combating of crime, e.g., the 2011 expert report of the Max Planck Institute for Foreign and International Law or the December 2019 analysis by the European Parliamentary Research Service on "general data retention/effect on crime."

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