Data Retention

Between Fundamental Rights and Integration

Lukas Martin Landerer

27.11.2024 doi: 10.59704/441ed897efb3bf32

The most vocally debated and legally intensively examined instrument of mass surveillance is the obligation of telecommunication services providers to retain metadata (such as traffic and location data or IP addresses) of all their users without them being in any way connected to a crime. The central protagonist in this saga of "mass data retention" is the Court of Justice of the European Union (CJEU). In its *Digital Rights Ireland* ruling of 2014, the CJEU declared the European directive (2006/24/EC), which universally obliged providers to retain their customer's traffic data, as incompatible with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (EU-CFR). Since then, the CJEU has granted Member States increasingly broad leeway in a series of rulings. Most recently, the Court ruled that the retention of IP addresses is permissible to combat "general criminal offenses".

This development has drawn criticism of the CJEU. Some argue that the Court has taken "one step forward and two steps back". First, the court wanted to establish itself as a highly fundamental rights sensible institution in *Digital Rights Ireland*. Then, in a "Copernican revolution", it revised its liberal stance. While I do not want to dismiss completely this criticism, I believe that one should not regard the court's shift as yielding to the political pressure from the Member States. Rather, it is the logical consequence of the expanding European competence on (constitutional) security law. Security law, in this context, refers to the law focusing on the procedures and investigation measures of law enforcement agencies and intelligence services. This traditionally nationally regulated legal field has become increasingly complex. Nowadays, constitutional courts do not strictly prohibit security measures, such as mass surveillance measures, but "procedural-ize" them.

The CJEU as both a "engine of integration" and fundamental rights institution?

If one had conducted a survey among lawyers and (other) social scientists in the early 2010s about what guides the CJEU in its decisions, the majority would likely have invoked the image of the "engine of integration". This phrase was often used – somewhat critically – to suggest that the CJEU tended to interpret European law more expansively than one could have expected by an objective instance. And as the Member States would have appreciated.

With the 2014 *Digital Rights Ireland* ruling, the CJEU assumed a new role, according to many observers. Unlike the German Federal Constitutional Court (BVerfG) four years earlier, the Court ruled that the obligation of private telecommunications providers to retain traffic data universally for six months and to hand it over to state security authorities was disproportionate. This decision was warmly welcomed in Germany, especially by politicians from the German-speaking world (such as former Justice Minister Sabine Leutheusser-Schnarrenberger and former Pirate Party member Patrick Breyer), who had sharply criticized the data retention obligation for its infringement on telecommunications privacy. According to prevailing opinion, the CJEU had established itself as a "fundamental rights institution" with the decision. Some even called it a "turning point in European fundamental rights protection".

The ban on data retention and its exceptions

Consequently, the reactions in the German-speaking discourse to the subsequent CJEU rulings on data

retention were rather negative, as these rulings gradually expanded the possibilities for national legislators to introduce data retention regulations.

In *Digital Rights Ireland*, the CJEU had already hinted at the permissibility of a limited data retention obligation. The main condition, according to the Court, was whether the stored data could potentially be used for crime prevention (para. 59). This opened up some flexibility for Member States, which then introduced national data retention laws.

The CJEU first clarified the requirements for proportional data retention in its ruling on the UK's and Sweden's data retention laws (*Tele2Sverige & Privacy International* (2016)). Later, while reviewing the regulations in France, Belgium and Germany (*La Quadrature du Net I* (2020), *SpaceNet* (2022) and *La Quadrature du Net II* (2024)), it progressively expanded the leeway available to Member States.

Some critics had believed that data retention was "stone dead" after *Tele2Sverige* because the boundaries set by the CJEU were extremely narrow. This interpretation, however, did not hold: data retention is today as alive as ever.

Since *La Quadrature du Net I*, the CJEU has allowed the universal retention of IP-addresses (yet initially only to combat serious criminal offenses). It has also allowed the retention of traffic data under two exceptions. These are

1. The universal retention of traffic data on a states' territory for short periods, when the member state is facing a serious, real, and ongoing or foreseeable threat to national security.
2. A "targeted data retention" in specific, particularly crime-prone areas, even without a national security threat.

Member States have creatively exploited these exceptions. France continues to implement a general data retention obligation nationwide, arguing that the national security threat required by the CJEU is continually present. It imposes a (short-term) data retention obligation on a rotating basis. The French Constitutional Court has essentially approved this practice. It was under significant pressure, since the French government threatened to pursue an ultra-vires review, if the court decided otherwise.

Belgium bases its national data retention on the "targeted retention" exception. The specific, crime-affected area where the data retention applies (without a national security threat) has, however, the same borders as the Belgian state territory.

The CJEU seems to have underestimated the resistance of some Member States to the ban on data retention. It was probably unaware of how differently security authorities use this instrument. French law enforcement agencies, for example, work much more intensively with traffic data than their German counterparts. According to a survey, French security authorities requested traffic data in over 80% of investigations in 2018-2019 (Commission study, p. 63). Thus, a data retention ban would particularly affect France.

Security law between integration and fundamental rights

According to Article 4(2) of the EU Treaty (TFEU), national security remains the sole responsibility of the Member States. The EU only has competence in criminal matters that typically have a cross-border nature. This competence however, primarily concerns the harmonisation of the definitions of criminal offence, not the national law enforcement authorities' investigation measures. Consequently, some argued after the annulment of the Data Retention Directive (DRD) that the EU-CFR could no longer apply to national obligations since there was no EU law requiring data retention anymore (England and Wales Court of Appeal, paras. 72 ff.).

The competence of the EU institutions over security law arises from the fact that security law today is primarily information law. European institutions use this vehicle to influence national investigative measures.

The CJEU based its authority in *Tele2Sverige* (paras. 73 ff.) on Article 15(1) of the E-Privacy Directive (2002/58). This provision states that the retention of telecommunications traffic data is generally prohibited unless it is necessary and appropriate for national or public security. The impact of this rule on national

data retention regimes was questioned, as the E-Privacy Directive does not apply to measures in the area of public security according to Article 1(3). However, the CJEU argued that Article 15(1) had no use unless it regulated national data retention regimes. Thereby, it established its competence over the issue. Some have argued that the Union lacks the competence to establish such a fundamental ban for national regulations in the field of security law in the first place (Wollenschläger/Krönke, NJW 2016, p. 906 (907 f.)). However, the CJEU had already commented on this issue of competence before:

The Commission has consistently argued that the data is not retained by state authorities, but by private companies. Therefore, it can rely on its competence to harmonize the internal market (Article 114(1) TFEU). In its decision on the passenger data agreement with the United States in 2006, the CJEU initially rejected the Commission's argument. The data transfer would obviously concern public security and state activities in criminal matters (paras. 57 and 54 ff.). Therefore, it was clear that the agreement did not mean to harmonize the internal market. However, in later decisions on the retention of telecommunications traffic data, the CJEU accepted the Commission's view (cf. critical remarks by Ambos 2009).

This explains why the CJEU considers Article 15(1) of the E-Privacy Directive to be a legal basis for a legitimate EU limitation on national data retention regimes. The Commission and the CJEU have expanded the scope of EU law factually to a broad range of security authorities' measures by treating the obligation of private entities to process data in this regard as a matter of market harmonisation. By doing so, the CJEU has put itself in a difficult position. It must harmonize procedures of national security authorities, although it is not originally competent for national security law.

"Proceduralized" security law

The CJEU had to find a way out of this situation. It appears to have aligned its case law to the jurisprudence of the Federal Constitutional Court of Germany (FCC).

Rather than declaring specific security measures as disproportionate, as the CJEU attempted in *Digital Rights Ireland*, the FCC derives specific thresholds and other requirements for surveillance and other security measures from the principle of proportionality. It has developed a broad catalogue of characteristics to define the intensity of any investigation measure. Based on this, the FCC classifies measures as on a scale ranging from "insignificant" to "very intense" using a firmly established case-by-case model. The entire system is so complex that it is referred to as an independent "constitutional security law", which no longer has much in common with a proportionality test in the sense of a rationality review (Poscher, Hdb. Verfassungsrecht, 2021, § 3, para. 82). Indeed, some have criticized recent decisions (e.g., the latest on the BKA-Act) as overstepping judicial boundaries by writing "guidelines" for legislation (cf. the dissenting opinion of Judge Schluckebier2010, para. 326).

The resemblance of the FCC's approach in recent rulings of then CJEU is clear. Thus, I do not regard the recent data retention rulings as signs of a growing authoritarian or "illiberal" jurisprudence. Rather, they are an advancement in terms of complexity and differentiation (cf. Eskens 2022). The Court has adopted a systematic approach, categorizing security law measures — much like the FCC — according to intensity levels and constituted specific conditions and thresholds for the legal basis of any security measure depending on its intensity (see this overview). The black or white thinking, which considers mass surveillance and other investigative measures generally as either proportionate or disproportionate, is outdated. Instead, these measures are "proceduralized".

The changing role of the fundamental rights institution

Therefore, one should not accuse the CJEU of abandoning its role as a sensible "fundamental rights institution". Rather, the CJEU has adopted the approach of other courts in the area of (constitutional) security law. As a European court, the CJEU cannot simply ban certain police measures, but must respect the complexity and heterogeneity of national law enforcement

agencies. Expanding the court's competence to prescribe rules concerning national security law would otherwise have led to significant conflicts with the Member States, as evidenced by the French government's open threat of an "ultra-vires review."

The CJEU's case law therefore does not reflect a shift towards a more fundamental rights-hostile interpretation of the law, but rather rests on the fact that the CJEU had to keep pace with developments in fundamental rights jurisprudence—at least in the area of security law.

ABOUT THE AUTHOR

Lukas Martin Landerer
Lukas Martin Landerer is a Lawyer for Public Law at W2K Rechtsanwälte based in Freiburg.

SUGGESTED CITATION

Landerer, Lukas Martin: Data Retention: Between Fundamental Rights and Integration, Verfassungsblog, 27.11.2024, doi: 10.59704/441ed897efb3bf32.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20241128-000258-0.