AG: Data Retention Should Be Strictly Limited

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

ISSN: 1862-6947
https://eucrim.eu

Advocate General (AG) *Manuel Campos Sánchez-Bordona* advocates that the CJEU's rather restrictive case law on the retention of personal data and access to these data by law enforcement or intelligence authorities should be upheld. Following the judgment in the Joined Cases C-203/15, *Tele2 Sverige,* and C-698/15, *Tom Watson and Others* (see eucrim 4/2016, p. 164), the CJEU now has to deal with further references for preliminary rulings. The AG's opinion is linked to references initiated by national courts in France, Belgium, and the UK. All seek clarification as to whether their national legislation on data retention is in line with EU law. The courts criticised the CJEU for having established hurdles that are too high; the requirements set out in *Tele2 Sverige/Watson* deprive the EU Member States of an instrument that is absolutely necessary in order to combat terrorism and safeguard national security, thus putting corresponding national security measures at risk. The references are as follows:

- Case C-623/17: Request for a preliminary ruling from the Investigatory Powers Tribunal (UK) in the case *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*. The main proceedings at the referring court concern the acquisition and use of bulk communications data by the United Kingdom Security and Intelligence Agencies (SIAs) via the operators of public electronic communications networks for the purpose of protecting national security, e.g., in the fields of counter-terrorism, counter-espionage, and counter-nuclear proliferation.
- Joined Cases C-511/18 and 512/18: both requests for a preliminary ruling came from the Conseil d'État (France) in the cases *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, Ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées*. The Conseil d'État essentially seeks clarification as to whether two obligations imposed on telecommunication service providers under French legislation are compatible with EU law: i.e., a) the (real-time) collection of specific data; b) the retention of location and traffic data in order to facilitate identification of any person who is civilly and criminally liable.
- Case C-520/18: Request for a preliminary ruling from the Cour constitutionnelle (Belgium) in the case: *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministres*. The Belgian court wonders whether the Belgian rules on the retention of data which follow multiple objectives (e.g. including the investigation, detection and prosecution of offences other than serious crime and the attainment of the defence of the territory and of public security) are compatible with EU law. In addition, the referring court asks whether it might maintain the effects of the national law on a temporary basis if a failure with EU law is concluded.

Although the AG issued three separate opinions, he clarifies that all cases before the CJEU raise common problems. In essence, the yardstick for all cases is Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and the fundamental rights enshrined in the CFR.

First, the AG examines the applicability of Directive 2002/58/EC. Although Art. 1 para. 3 of the Directive excludes from its scope "activities concerning public security, defence, State security (…) and the activities of the State in areas of criminal law," the AG concludes that this exemption only refers to specific activities by the State authorities on their own account. In data retention situations, however, obligations are imposed on private parties, whose cooperation is required. Even if this cooperation is required for national security interests, these activities are governed by the Directive, i.e., the protection of privacy, which is enforceable against private actors. Accordingly, Directive 2002/58 is applicable in the data retention scenarios.

Second, the AG deals with the possibility under Art. 15 para. 1 of Directive 2002/58. Under certain conditions, it allows Member States to adopt legislative measures providing for the retention of data if these measures follow objectives of safeguarding national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. Limitations to the privacy rights enshrined in the Directive (in particular, the guarantee of confidentiality of communications and related traffic data) must be interpreted strictly and with regard to the fundamental rights enshrined in the CFR. The AG proposes upholding the case law of the judgment *Tele2 Sverige /Watson*. From the Union law perspective, it is disproportionate and unlawful if national laws establish a general and indiscriminate retention of all traffic and location data of all subscribers and registered users. By contrast, a Member State can follow the approach of limited and discriminate retention flanked with limited access to said data. This would entail the following aspects:

- Retention of specific categories of data that are absolutely essential for the effective prevention and control of crime and the safeguarding of national security;
- Retention for a determinate period adapted to each particular category;
- Data access subject to a prior review carried out either by a court or by an independent administrative authority;
- Notification of data subjects (provided that ongoing investigations are not jeapordised);
- Adoption of rules to avoid misuse of, and unlawful access to, retained data.

The AG stressed, however, that it is not the task of the CJEU to develop a lawful data retention model. This must be done by the legislator.

Further developing the previous case law, the AG suggests that imposing a more extensive and general data retention regime is possible for "exceptional situations characterised by an imminent threat or an extraordinary risk warranting the official declaration of a state of emergency." However, such a regime can also only be lawful for a limited period and it must be proportionate.

As regards the concrete cases at issue, the AG concludes that Union law precludes the established national data retention legislations in France, Belgium, and the UK, because they are general and indiscriminate. There is, however, no preclusion for the specific part of French law that permits the real-time collection of traffic and location data of individuals, "provided that those activities are carried out in accordance with established procedures for accessing legitimately retained personal data and are subject to the same safeguards."

As regards the specific question posed by the Belgian court, the AG proposes that "a national court may, if its domestic law so permits, maintain the effects of legislation such as the Belgian legislation, on an exceptional and temporary basis, even where that legislation is incompatible with EU law, if maintaining those effects

is justified by overriding considerations relating to threats to public security or national security that cannot be addressed by other means or other alternatives, but only for as long as is strictly necessary to correct the incompatibility with EU law."

If the CJEU follows the opinion of AG *Campos Sánchez-Bordona,* the cases at issue may have an impact on other jurisdictions. This includes the request for a preliminary ruling by the Federal Administrative Court of Germany asking for verification of the lawfulness of the 2015 German law on data retention (see eucrim 3/2019, p. 176). On 21 January 2020, AG *Pitruzzella* also published his opinion on interpretation of the Estonian data retention legislation (see separate news item).

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