CONSEIL D'ÉTAT

Paris, 21 avril 2021

PRESS RELEASE

Connection data: the Council of State conciliates the implementation of European Union law and the effectiveness of the fight against terrorism and crime

Ruling on appeals lodged by several NGOs and a telecom operator, the Council of State has examined the conformity with EU law of French rules on the retention of connection data. It also verified that the implementation of EU law, as interpreted by the European Court of Justice (ECJ) does not jeopardize the requirements of the French Constitution.

The Council of State rules that the existing threat to national security currently justifies the generalized retention of data. It also notes that the possibility of accessing connection data in order to fight serious crime allows, at the present time, the constitutional requirements of preventing breaches of law and order and the tracking down of authors of criminal offences to be ensured.

However, it orders the Government to reassess regularly the threat that exists in France so as to justify the generalized retention of data and to submit the use of these data by the intelligence services to clearance provided by an independent authority.

French law requires telecommunications operators to retain their users' connection data for the purpose of fighting crime and terrorism

The use of connection data plays a major role in the search for criminal offences and in the activities of intelligence services, particularly in order to fight terrorism. This data, sometimes referred to as "metadata" to differentiate it from data which relate to the content of exchanges, include three categories:

- identity data, which allows the identification of the user of an electronic communication system (for example, the first and last names linked to a telephone number or the IP address through which a user is connected to the internet);

- traffic data (sometimes called "*fadettes*"), which track the dates, hours and recipients of electronic communications, or the list of websites consulted;

- location data, which allows a device to be "marked" by the base station to which it is connected.

French law requires communications operators to retain all users' connection data for intelligence and criminal investigations purposes.

The ECJ has strictly limited the possibility of requiring operators to retain connection data

Several NGOs (*associations*) active in the field of data protection and a telecom operator had lodged appeals before the Council of State against the decrees that provide for such retention and govern their processing for the purposes of intelligence and criminal investigations.

Such appeals enabled the Council of State to refer the matter to the ECJ in 2018[1], so as to invite it to clarify the effect of relevant EU rules (Directive 2002/58, known as "privacy and electronic communications" and GDPR). Several courts of other Member States also referred cases to the ECJ for the same purpose. In a judgment dated 6 October 2020[2] joining three cases, the ECJ gave details on the limits, which, in its view, are set by the EU legislative framework.

1) A Member State can only require providers of electronic communication services to generally retain traffic and location data in situations where this is needed as a result of a serious threat to national security. Furthermore, access to this data by the intelligence services is subject to prior review by an independent administrative body and subsequent judicial control on the use of stored data.

2) For the purposes of combating serious crime, States may impose only targeted retention of data, in certain areas or on certain categories of persons pre-identified as raising particular risks. However, as provided for by the Budapest Convention of 2001, public authorities can demand that operators freeze traffic and location data relating to a person, for the purposes of a criminal investigation and for a short period of time (the so-called "expedited data retention" method).

3) Retention of connection data is not allowed on other grounds, notably for the investigation of offences which do not involve serious criminality.

The Council of State checks that the implementation of EU law does not jeopardize French constitutional requirements

Following the clarifications made by the ECJ, the Council of State, sitting in its highest jurisdictional body (Assemblée du contentieux), had to examine the conformity of the French legal framework with EU law.

---

[1] CE, 26 juillet 2018, Quadrature du Net et autres et Igwan.net, n°s 394922 394925 397844 397851, T.

[2] ECJ, 6 October 2020, *Privacy International*, aff. C-623/17 ; *La Quadrature du Net e.a., French Data Network e.a.*, aff. C-511/18 et C-512/18 ; *Ordre des barreaux francophones et germanophone e.a.*, aff. C-520/18.

First it clarified the scope of its review.

On the one hand, and contrarily to the Government's request, it refused to assess whether the European Union authorities, notably the ECJ, had exceeded their powers ("ultra vires" review).

On the other hand, the Council of State recalls that the French Constitution remains the supreme norm within the French national legal system.

Consequently, the Council of State must ensure that the application of EU law, as specified by the ECJ, does not in practice jeopardize French constitutional requirements which are not guaranteed in an equivalent manner by EU law.

The European legal framework of data retention does not collide with the French constitutional requirements related to security and fight against crime.

The Council of State notes that the constitutional requirements of safeguarding the fundamental interests of the nation, preventing breaches of law and order , fighting against terrorism and searching for the perpetrators of criminal offences do not enjoy a protection in EU law equivalent to that guaranteed by the French Constitution. The Council of State must therefore ensure that the limits imposed by the ECJ do not jeopardize these constitutional requirements.

The Council of State notes that the general retention of data currently imposed on operators by French law is actually justified by a threat to national security, as required by the ECJ. Following the ECJ's requirements, it requires the Government to assess from time to time the existence of such a threat, subject to review by administrative courts.

However, the Council of State rules that the generalized obligation to retain data for purposes other than those of national security, notably the prosecution of criminal offences, is unlawful (with the exception of less sensitive data, such as civil status, IP address, accounts and payments).

For the prosecution of criminal offences, the ECJ's suggested solution of targeted upstream data retention is neither possible in practise nor operationally effective. Indeed, it is neither possible to pre-designate those who will be involved in a crime still not committed, nor the place where it will take place. However, the method of "expedited retention" permitted by EU law can build on the stock of data generally retained for national security purposes and thus be used for the prosecution of criminal offences.

With regard to the distinction made by the European Court of Justice between serious crime and ordinary crime (for the latter of which it does not admit any retention or use of

connection data), the Council of State recalls that the principle of proportionality between the seriousness of the offence and the importance of the investigative measures used, which governs criminal procedure, also justifies that recourse to connection data is limited to the prosecution of offences of a sufficiently serious nature.

Finally, with regard to the use of retained data for intelligence purposes, the Council of State notes that the prior review by an independent authority provided by the French legal framework is not sufficient because the opinion of the National Commission for the Control of Intelligence Techniques (CNCTR), which must be given prior to any authorisation, is not binding. Even though the Prime Minister has never refused to follow an opinion of this Commission recommending refusal of access to connection data by the intelligence services, French law should be amended on this point.

The Council of State therefore orders the Prime Minister to modify the regulatory framework to comply with these requirements within six months.