Case law on the retention of communications data and its impact on national legislation and criminal proceedings - The French case

Speech by Mr Rémy HEITZ,

Public Prosecutor at the Court of Cassation, 27 May 2024

Distinguished Prosecutors General, dear colleagues,

I too would like to extend my warmest thanks to the Luxembourg Presidency, dear Martine, for its welcome and for the perfect organisation of this 15th meeting of the Network of Prosecutors General of the European Union.

As head of the General Prosecutor's Office of the French Court of Cassation for less than a year, this is the first time I have attended this meeting, which is an opportunity to get to know a large number of partners. I have high expectations of our Network, to which I hope to make a full contribution.

In this, my first speech, I am delighted to be able to talk about a key issue, that of connection data. This is a subject that has been of common interest to our public prosecutors' offices for more than 10 years, and one that has become increasingly important as our lives have gone digital.

As a corollary, connection data has become ubiquitous in criminal investigations, whether used for the prosecution or the defence.

This is all the truer now that cybercrime has been added to traditional delinquency. For these offences committed online, metadata are the only evidence available.

But this connection data is also a potential threat to citizens' freedoms, a possible invasion of their privacy by national authorities.

It is with this in mind that the case law of the CJEU has been built around two main principles: A ban on the general and indiscriminate retention of traffic and location data, except, exceptionally, where there is a serious threat to national security. Prior control by a court or an independent authority of access to such data in the context of investigations.

This case law, in many of our countries, came as a surprise at first and then became the subject of controversy. A French Senate report described it as a ‘procedural shock’ for both investigating authorities and public prosecutors.

For their part, legislators have had to question themselves and take action. They have sometimes done so belatedly, in several stages, and without necessarily completing their work today. It has to be said that there is absolutely nothing obvious about the solution to be found, as national authorities are caught in a vice between, on the one hand, organised crime, which is destabilising and tentacular, and, on the other hand, mass surveillance, which is liberticidal, with data as a weapon for each of them.

So this morning we are dealing with a subject that is both arid, technically highly complex, decisive for our investigations and politically sensitive.

Against this delicate backdrop, the case law of our highest national courts has followed on from that of the CJEU, while at the same time prompting the Court to clarify its position through the many preliminary questions it has been asked. They have also highlighted the issues surrounding the interaction of this case law with that of the ECHR.

So what is the situation with French legislation and case law on the retention of connection data, firstly, and access to such data, secondly?

1/ With regard to data retention, it should be remembered that the CJEU, in its La Quadrature du Net decision of 6 October 2020 , ruled that French legislation could not impose a general and undifferentiated retention of traffic and location data on electronic communications operators and Internet access providers as a preventive measure, without at the same time justifying a threat to national security.

For its part, the French Constitutional Council ruled that the general and indiscriminate retention of such data was unconstitutional.

In four rulings handed down on 12 July 2022, the Criminal Division of the French Supreme Court (Cour de cassation) was called upon to rule on the issue within the French judicial system, drawing the consequences of these decisions and clarifying the conditions under which French law complies with EU law.

Like the CJEU, the Court drew a distinction between the categories of connection data according to the degree of invasion of privacy, applying a strict legal regime to traffic and location data, to which I will now turn.

With regard to the general and indiscriminate storage of such data, the Cour de cassation ruled out the application of legislative and regulatory provisions that provided for such data to be stored as a preventive measure to combat crime.

On the other hand, it upheld the application of the text that required it on the grounds of the serious, actual and present or foreseeable threat to which France has been exposed since December 1994 as a result of terrorism and the activities of radical and extremist groups.

On this basis, and in compliance with European law, French law continues to allow the Prime Minister to order electronic communications operators to retain this data for a period of one year.

This is a power that the regulatory authorities are continually seizing upon, to enable our country to deal with a threat that everyone knows to be serious and long-lasting.

Once this data has been retained for a reason unrelated to the fight against crime, the question arises as to the conditions under which the judicial authorities can access it in the course of their investigations.

2/ This is the second stage of the reasoning, that of judicial access to connection data.

This access is not prohibited by EU law, but is subject to two conditions: firstly, a necessity test, and secondly, prior and independent control.

As regards the criterion of necessity, the Cour de cassation has once again drawn the consequences of European law to require that such access does not go beyond what is, from a material or temporal point of view, strictly necessary for the prevention or punishment of the offence concerned. Requiring effective control in this area, it ruled that this was not the case in the case of requisitions issued by an investigating judge in execution of a general letter rogatory.

Our law therefore imposes a criterion of genuine necessity. This criterion depends on the specific features of each procedure, but first and foremost on whether the offence in question is sufficiently serious.

In this respect, the CJEU ruled a few days ago that the definition of 'serious offences' falls within the competence of the Member States when defining the scope of access to such data. It did, however, specify that setting a quantum of the penalty incurred was a relevant objective criterion, ruling that a threshold set by reference to a maximum sentence of three years' imprisonment did not appear to be excessively low.

This is a reassuring decision in terms of the conventionality of French law, since our legislature had, as early as March 2022, broadly restricted the requisitions allowing such access to proceedings involving an offence punishable by at least three years' imprisonment.

Referring to the state of the law prior to this legislative change, the Court of Cassation, in its rulings of 12 July 2022, transposed the general requirement laid down by the CJEU, ruling that it is up to a court hearing a case challenging the lawfulness of access to such data to verify that the offence in question falls within the scope of serious crime.

This concept has been clarified by the High Court, which has set out assessment criteria designed to help those carrying out such checks, not only a posteriori, but also a priori.

Referring to this a priori verification, I now come to the other condition laid down by European law, which has posed more difficulty in French law: the determination of the authority responsible for carrying out prior control of this access.

In this respect, the Cour de cassation has once again drawn the consequences of the CJEU's rulings by ruling out the application of several articles of the Code of Criminal Procedure which did not provide for a prior control by a court or an independent administrative body in the context of investigations conducted under the authority of the public prosecutor.

However, the Court of Cassation made the nullity of proceedings carried out in such an irregular manner subject to proof of the existence of unjustified interference in the private life of the person concerned.

In other words, it required the applicant to prove that an actual grievance had resulted, by establishing that a prior check would have revealed that the conditions for such access had not been met.

The Court of Cassation reiterated this case law very recently, in a ruling dated 27 February 2024 , extending its application to real-time geolocation of a mobile phone.

Based on this interpretation, French public prosecutors have continued to issue requisitions for access to connection data in investigations conducted under their authority, while strengthening their prior control to ensure that the person concerned has not been harmed. This practice, which has been upheld by the Paris Court of Appeal, has made it possible to preserve an essential balance while awaiting a legislative change that will mobilise the authority required by the CJEU.

***

So there is an abundance of case law, interweaving the decisions of national and European courts, in a body of law that continues to evolve, particularly as a result of a large number of preliminary questions, but also as a result of referrals by citizens in relation to the ECHR.

National legislators sometimes intervene to draw the consequences of the decisions of our courts. In France, the Senate is hoping for new legislation within 2 or 3 years, which corresponds to the deadline set for the overhaul of our code of criminal procedure.

But the authorities are moving forward on shaky ground, while the overall solution lies at European level. In this context, it is to be hoped that the European negotiations will result in a compromise that guarantees not only freedoms but also the effectiveness of criminal investigations.

In any event, and to end on a positive note, we can be pleased that these cases have highlighted the importance of coordinating our legislation and our actions, and that they have given rise to a profound reflection on the need for a common system of digital evidence and, more broadly, a coherent system of control for criminal investigations.

Thank you for your attention.