Criminal investigation: retention of and access to connection data

12/07/2022

Appeals n° 21-83.710, 21-83.820, 21-84.096 and 20-86.652

The Court of cassation draws the consequences of the decisions delivered by the Court of Justice of the European Union concerning the retention of connection data and access to them in the context of criminal proceedings.

Warning: *this press release is not intended to set out in full the content of the decisions. It aims to present a summary of their main legal inputs.*

European Union law: protection of privacy, personal data and freedom of expression

General rule

Member States of the European Union shall not impose on electronic communications operators, Internet access providers and hosting companies to retain, generally and indiscriminately, all traffic and location data.

Exceptions

Such retention may take place, under certain conditions, in case of a serious and current threat to national security.

In order to solve a specific serious crime, Member States may also require operators and providers to retain data "expeditiously" if they provide certain guarantees.

Access to the retained data shall, in any case, be authorized by a court or an independent administrative body.

What kind of connection data are concerned?

These are:

- **traffic data**, establishing the contacts a person has had by phone or SMS/the date and time of these contacts /the duration of the exchange;
- **location data**, allowing to know the transmission and reception areas of a communication made with an identified cell phone/obtain the list of calls having terminated at the same relay antenna.

These data are available on the so-called "*fadettes*".

Background

According the Court of Justice of the European Union, these data « may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health [...].

Taken as a whole, **those data may allow very precise conclusions to be drawn concerning the private lives of the persons** whose data have been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them »

Facts and procedure

In several cases, including murder and drug trafficking, the accused persons (*personnes mises en examen*) sought the **annulment of judicial requisitions** (*réquisitions*) relating to their traffic and location data, issued by investigators acting in flagrante delicto under the supervision of the public prosecutor or on the basis of a letter rogatory from the investigating judge, as well as of the acts of **use of these data**.

According to the applicants, these data had been subject to:

- an irregular retention because the French legislation in force at the time required operators to retain all connection data for one year for the investigation of all criminal offenses;

- an irregular access because the personal data was obtained by the investigators with the authorization of the public prosecutor or the investigating judge, who are neither a court nor an independent administrative body.

Principles

Background

In order to guarantee the effectiveness of EU law in the various Member States, the national court must interpret French law in a manner consistent with EU law.

In the absence of such an interpretation, the national court shall leave unapplied the rules of French law that are contrary to EU law.

If the judge does not respect the legislation of the European Union, he or she exposes the State to an action for failure to comply (recours en manquement).

General retention of traffic and location data (Applicable regime prior to the law of 30 July 2021)

The safeguarding of national security allowed for a general and undifferentiated retention of data.

The French regulation, insofar as it provided for the general retention of connection data for the **protection of the fundamental interests of the Nation** and the **fight against terrorism**, was in conformity with EU law, subject to a periodic review of the existence of a serious threat to national security.

In the cases examined, a threat to national security existed before the facts: this is what emerges from the documents produced by the Prosecutor-General of the Court of cassation relating to the **attacks committed in France since December 1994**. The one-year retention period is considered strictly necessary to safeguard national security.

However, the general retention for other purposes was contrary to EU law.

It was possible to order, by judicial requisitions (*réquisitions*), the "expedited" retention (*quick freeze)* of data to solve a serious offence and in so far as is strictly necessary: in case of dispute, the judge seized must assess the necessity of the retention.

The data retained by the operators for their own needs or to safeguard national security, can also be retained, at the request of investigators, by way of judicial requisitions (*réquisitions*), for the punishment of a specific serious offence.

In this case, the judicial requisitions (*réquisitions*), are equivalent to an "**expedited" retention order**.

In order to ensure compliance with EU law, when a plea of nullity is brought before the court challenging the legality of the judicial requisitions, **the judge must check** that:

- the facts in question are **serious crimes** ;

- the "expedited" retention of connection data and access to them are limited to what is **strictly necessary**.

Access to traffic and location data

The investigating judge, who is a court, can control access to data; the public prosecutor, who is not a third party in the investigation, cannot do so.

The law, insofar as it allows the **public prosecutor** or an **investigato**r to access the data, is contrary to EU law because it does not provide for **prior review by a court or an independent administrative body**.

The public prosecutor directs the investigation procedure and, where appropriate, prosecutes the case: he or she is thus involved in the conduct of the criminal investigation and does not have a neutral stance vis-à-vis the parties to the criminal proceedings, as required by EU law.

However, the **investigating judge is entitled** to exercise this control, since he or she is not a party to the proceedings but a **court** and does not exercise the right of public prosecution.

Consequently, the accused (*personne mise en examen*) may, under certain conditions, invoke the violation of the requirement of independent control of access to his or her connection data.

The act that allowed access to the data can only be annulled by the judge if the privacy of the accused (*personne mise en examen*) has been violated and if the latter has suffered damages.

The Court of cassation clarifies the **consequences of irregular access to connection data** on the validity of investigative acts:

- The law gives the accused (*personne mise en examen*) the possibility to effectively challenge the relevance of the evidence derived from his or her data, in particular in the context of a request for an expert opinion.
- EU law seeks to protect privacy: not respecting it is tantamount to infringing a private interest. Therefore, the accused (*personne mise en examen*) can only invoke the violation of the requirements of data access control if he or she claims to be the **owner or user of an identified telephone line** or if he or she demonstrates that his or her **privacy has been violated** during these investigation.
- The criminal judge can only annul the acts that allowed access to the data if the irregularity observed has caused damages to the accused (*personne mise en examen*). Damages are established:

- when the data could not be retained under the "expedited" retention;
- or when the categories of data concerned and the duration during which it was possible to access them were not limited to what was **strictly necessary** for the proper conduct of the investigation in question.

The consequences in the cases examined

In cases where the accused (*personnes mise en examen*) had no rights to the telephone lines, the petition for nullity are deemed **inadmissible.**

In cases where the accused (*personnes mises en examen*) had a right to the telephone lines, the **appeals are dismissed** because:

1. The connection data was regularly retained since the facts were indeed **serious crimes** (murder in an organized gang, destruction by dangerous means, import and export of hundreds of kilos of drugs by an international criminal organization, etc.), and that the judicial requisitions (*réquisitions*) to the operators of the connection data (identity, traffic, location) and their use were necessary for the proper conduct of the investigations.

2. **Access** by investigators acting on a letter rogatory issued by the investigating judge was regularly granted.

3. Although investigators had **irregular** access to traffic and location data in the context of a flagrante delicto investigation conducted under the control of the public prosecutor, the investigating chamber of the court of appeal (*chambre de l'instruction*) was able to validly reject the petitions for nullity, because, **in this case**, the categories of data concerned and the duration during which it was possible to have access to them were limited to what was **strictly necessary for the proper conduct of the investigation**.

Press releases | Europe | Criminal law