FONDATION ROBERT SCHUMAN

POLICY PAPER

**European issues**
n°510
9th April 2019

# Protecting European citizens in an ultra-connected world

**François MOLINS**

On 3rd April last, the Robert Schuman Foundation organised a conference in Luxembourg with the Max Planck Institute on the theme "Protecting European citizens in a highly connected world". It was attended by eminent personalities representing the European institutions and in particular the Advocate General, Henrik Saugmandsgaard Øe, representing the President of the Court of Justice of the European Union.

A full report of this work will be published at a later date. We are already aware of the very interesting communication made by Mr François Molins, Attorney General at the Court of Cassation of the French Republic, former Prosecutor at the Paris Court and, as such, in charge of the fight against terrorism. In particular, it alerts on the needs of the services in charge of the fight against terrorism and serious crime, with regard to the storage and access to electronic data.

The following developments are the result of my 7 years' experience as head of the Paris Public Prosecutor's Office responsible for anti-terrorism and the fight against organised crime. In these two areas, we have to take into account several phenomena that constitute major challenges:

- In the field of terrorism, the threat is now sustainable and endogenous. It is the work of individuals, often with weak signals, who, adhering to Daesh's deadly theses and unable to reach the Iraqi-Syrian zone, may be tempted or inspired to act individually in accordance with the permanent watchwords of this terrorist organization. This threat is widespread and therefore all the more difficult to detect for the intelligence services of States.
- In the field of organised crime, criminal organisations are becoming increasingly professionalised and their leaders no longer need to go to the field to give their instructions. They use new technologies. The management of criminal operations is increasingly dematerialized and protected by encryption processes.
- Finally, the means of proof have evolved considerably. Electronic evidence resulting from connection and location data as well as content data from electronic exchanges are becoming increasingly important in judicial investigations and before criminal courts.

In the light of these reflections, I will focus mainly on the problem of the conservation of traffic and location data and the consequences of the current case law of the Court of Justice of the European Union.

Connection data, also known as metadata, or traffic and location data, does not refer to the content of messages, but to the conditions under which they were accessed or exchanged. They therefore relate to the identity and location of the author and recipient of communications, the date and duration of the communications, the materials, telephone numbers and IP addresses used. The exploitation of these data is based on their generalised, undifferentiated storage for a certain period of time by electronic communications operators, who are required to do so by law. To a certain extent, it makes it possible to read the past by tracing the activities in which an individual has engaged on the network even before being suspected of criminal activities, but also to read the present (geolocation).

For the State, it is therefore a very valuable weapon, particularly in the fight against the contemporary terrorist threat, the massive or diffuse nature of which is well known.

This is obvious in the fight against terrorism. In the case of organised crime, it is just as much so because today, the heads of criminal organisations are no longer subject to traditional surveillance methods. They no longer go to the field; they stay away and give instructions using new technologies.

On 21st December 2016, in a Tele 2 Sverige and Davis decision, which was widely commented on in terms of strengthening privacy protection, the European Court of Justice ruled that national legislation providing for generalised and undifferentiated storage of all traffic and location data and not sufficiently regulating their consultation by national authorities was not in conformity with Union law. The High Court thus holds that if data retention is possible, it must be targeted and

limited to what is strictly necessary. Access to this data may only be authorised by a judge or an independent administrative authority. This decision was clarified by a judgment of 2nd October 2018 Ministerio Fiscal C-207/16.

These requirements weaken national legislation, and in particular French legislation, with regard to the storage and access to connection data, both for intelligence services, which are nevertheless under the control of the National Commission for the Control of Intelligence Processing, and for judicial investigations, which are under the control of the judiciary.

However, these applicable principles are not stabilised since several preliminary questions are pending before the ECJ. They were put by the United Kingdom, by the Belgian Constitutional Court on 2nd August 2018, by the French Council of State on 26th July 2018 and finally by the Estonian Court on 29th November 2018. By these questions, the national courts invited the ECJ to clarify, in particular, whether the prohibition on generalised data retention should not be tempered by taking into account the seriousness of the threat (Council of State), and whether the prosecutor can be regarded as an independent administrative authority within the meaning of this expression given by the ECJ (Estonia).

If this Tele2 decision is confirmed, the impact of this case law on investigations into terrorism and organised crime can only be cause for serious concern. It is to be feared that the Luxembourg Court has not mastered how the services responsible for investigations manage to identify perpetrators of crimes or members of criminal networks, whose perfect mastery of police techniques leads them to "professionalise" the erasure of traditional traces and clues. Data retention and controlled but fluid access thus now appears to be the prerequisite for successful investigations in common law, organised crime and, of course, terrorism.

The general meaning of the above-mentioned decision and the Court's reading of Directive 2002/58 on the processing of personal data seem unambiguous: storage should only be very limited in its criminal scope - only for the purpose of combating serious crime - and in its material scope - limited to what is strictly necessary for data, persons and time.
The basis for the decision is based on Articles 7 (respect for private and family life), 8 (protection of personal data), 11 (freedom of expression) and 52 (respect for the principle of proportionality in infringements of rights) of the Charter of Fundamental Rights of the European Union. This is the core of the law of the Union and its democratic states.

However, the ability to combine the protection of these rights with those recognized in Articles 2 (right to life) and 6 (right to liberty and security) is not mentioned in the decision or in most of the comments made on it. The Court of Justice even seems to give relatively little weight to the general interest objective of the fight against terrorism, since in paragraph 103 of the Tele2 judgment, while explicitly recognising the effectiveness of general data retention, it considers that this is not sufficient to make this measure necessary.

However, this control of proportionality appears to be a fundamental question facing our society. In the digital age, the protection of privacy and personal data is one of the essential guarantees of our freedoms. But must it be so absolute, or must its limits be so constrained, that it would in fact take precedence over the ability of public authorities to protect the right to security and thus the exercise of all freedoms?

This is the question raised by the decision of the Court of Justice of the European Union in December 2016. If confirmed and the interpretation of the principles outlined therein were to be strict, the immediate consequence would be the end of many of the criminal investigations currently under way[or even the invalidity of acts already carried out], whether they concern acts of serious harm to ordinary persons - homicides, rapes -, offences relating to organised crime or acts of terrorism.

The Court's conditions for access to data appear to be poorly grounded in reality. The Court thus requires that "the retention of data must be, as regards the categories of data to be retained, the means of communication concerned, the persons concerned and the period of retention retained, limited to what is strictly necessary". The Court considers that these can be defined according to alternative criteria, by reference to a circle of suspected persons, a time period or a geographical area.

It's a pure construct of the mind!

In its implementation, this expectation means that there is no longer any retention of useful data.

By hypothesis, with the exception of investigations for criminal

association with nominal objectives, there is no crime for which the perpetrators would be known in advance and for which data retention could be ordered. It is obviously only after the fact, once the first elements of the survey have been collected, that the consultation of the stored data will be carried out. If there is no data stored beforehand, there is no consultation. The Tele2 Sverige and Davis decision of the European Court of Justice therefore appears to be based on a reasoning which, although legally understandable, is materially unrealistic.

Without prior retention of data, it is not possible, after a serious criminal act such as a terrorist act, to cross the connections between the persons involved and therefore to establish their participation in the facts or to identify their accomplices and dismantle the networks.

Login data is essential for investigations in both administrative and judicial settings. They are an essential "raw material" for judges and investigators.

With regard to telephone data, requests addressed to operators can be of two types:
- from a telephone number (recording of calls made and received, location of calls from the target, association with one or more boxes, etc.),
- from a telephone relay (reading of all the telephone numbers that triggered this relay in a given time slot).

These requests include, but are not limited to, the following:
- to locate a person or reconstruct the path of a person under surveillance,
- to determine a person's circle of relationships (relationships of an individual being monitored in a terrorism prevention framework),
- to detect the occurrence of atypical movements likely to shed light on an investigation.

Some examples of use:
- Counter-terrorism in the Iraqi-Syrian channels: the study of connection data made it possible to update contacts in Turkey and Syria and to identify the relationships that played a logistical role in departures to the area. This is evidence to identify an organized sector.
- The arrest in France of Mehdi Nemouche (assassinations of the Jewish Museum in Brussels on 24th May 2014) led the investigators to urgently request the available connection data in order to identify, from his environment, the possible existence of another project in France, as well as accomplices. The issue from a national security perspective was therefore essential.
- Attacks on Saint Denis and Bataclan on 13th November 2015. After these attacks, we had few clues. An image from the video surveillance device showed a terrorist who had blown himself up at the Stade de France on a mobile phone at 9:00 pm, and a mobile phone found by investigators in a garbage can located in front of the entrance to the Bataclan in Paris. The demarcation carried out from the telephone relay near the Stade de France made it possible to identify 15,094 telephone calls that activated this relay between 9;00 pm and 9. 04 pm. The analysis of these communications and the cross-referencing with the contents of the mobile phone box discovered in front of the Bataclan showed that they had both activated the same Belgian telephone chip. This has made it possible to guide judicial investigations. If we had not been able to immediately access this data on the connection and location of these mobile phones, the course of the investigation would have been considerably slowed down and the identification of terrorist cells in France and Belgium delayed or even stopped.
- in the case of the planned attack on the Villejuif church preceded by a deliberate homicide against a young woman, the analysis of the Internet activity determined that the alleged perpetrator had received his instructions from a third party based abroad.
- Elucidation of murder (case of Hélène Pastor in Monaco). The considerable analytical work carried out on the basis of 3.5 million telephone calls was decisive in identifying the perpetrators. The same applies to the case of Nordahl Lelandais, suspected of having committed a deliberate murder on a 10-year-old child and then on a French army soldier.
- Finally, the analysis of Internet connection data is essential to detect pornographic images of children and arrest those that put content online or acquire it.

Obtaining this "metadata" is therefore a valuable and indispensable weapon in the fight against serious crime and particularly the contemporary terrorist threat. The system for the systematic collection of "metadata" is therefore of crucial importance in protecting national security. Without it, in an administrative context, the intelligence services would be deprived of all the history and in a judicial context, everything would depend on the ability of the authorities to anticipate the identity of persons whose connection data could be useful, which is impossible.

Finally, the case law of the Court of Justice differs from that of the European Court of Strasbourg and therefore creates a situation of legal uncertainty since, in its recent developments, the European Court of Human Rights has concluded in particular that the use of a mass interception regime does not in itself constitute a violation of the Convention. (ECHR Centrum för Rättsiva v. Sweden of 19th June 2018 and Big Brother Watch v. United Kingdom of 13th September 2018). At the very least, Member States should be subject to convergent criteria for assessing the need and the proportionality of the technique of supervision depending on whether the interference is examined in the light of the European Convention or the Charter of Fundamental Rights.

The legal choice for our democracies cannot be privacy protection versus arresting criminals and terrorists. The legal choice must be that of protecting privacy by ensuring that there is judicial access to the data stored. The prevention of breaches of public order is indeed necessary to safeguard the rights and exercise the freedoms of our fellow citizens.

For judicial investigations, the authorisation of access to data of particular sensitivity must be granted by the judicial authorities, which in our democracies are the guarantors of individual freedoms. The existing judicial mechanisms in the Member States of the Union must make it possible to find the essential framework for ensuring control and effectiveness without falling into the trap of making criminal investigations of a level of legal complexity that undermines their effectiveness.

The balance to be struck is delicate, but caricatured protection of personal data will immediately lead to a weakening of the authorities responsible for identifying and prosecuting the perpetrators of crimes. In a democracy, it is the state and its authorities that are responsible for protecting fundamental freedoms. This principle seems to me to be the guarantee of an optimal functioning of our institutions. The European Court of Human Rights has underlined this principle by ruling that "proactive obligation of Contracting States to guarantee the protection of privacy implies the obligation to give judicial authorities the possibility of accessing dynamic IP addresses and communication data in order to identify a private person who has violated another individual's right to privacy"; (ECHR, Case K. U. v. Finland, 2nd December 2008, No 2872/02)

In conclusion, it seems to me that a real reflection must be undertaken with regard to all these challenges and to the responsibilities of each institution to ensure that these imperatives are reconciled.

The dialogue between judges is certainly essential to achieve this, bearing in mind the premonitory conclusions of the Government Commissioner Bruno Genevoix, who recalled in 1978 that "at the level of the European Community, there must be neither a government of judges nor a war of judges. There must be room for dialogue between judges".

**François Molins**

Attorney General at the Court of Cassation of the French Republic, former Prosecutor at the Paris Court and, as such, in charge of the fight against terrorism.

You can read all of our publications on our site :
**www.robert-schuman.eu**
Publishing Director : Pascale JOANNIN