DIGITAL EVIDENCE IN CRIMINAL LAW

Olivier GUTKÈS

In French criminal law, "Except where the law otherwise provides, offences may be proved by any mode of evidence and the judge decides according to his innermost conviction" (Article 427 of the Code of Criminal Procedure).

Digital evidence is therefore admissible in the same capacity as all other modes of proof.

Thus, computer science plays naturally an increasingly larger part in the production of evidence in criminal law.

Indeed, computer science has become a mean to support the search for evidence (1) as well as evidence in its own right (2).

1. COMPUTING SCIENCE AS A MEAN TO SUPPORT THE SEARCH FOR EVIDENCE

In response to the development of cyber criminality, computer science has become an essential mean in the search for evidence; either through digital infiltrations (1.1) or through remote data captures (2.2).

1.1 Digital infiltrations

Since the entry into force of the Laws of 5 March 2007 and of 14 March 2011, infiltrations through the Internet network are possible in matters such as the fight against terrorism, trafficking in human beings, procuring, resorting to the prostitution of minors, child pornography and more widely in any case of endangerment of minors.

With the aim of finding those criminal infringements, gathering evidence and apprehending offenders, the police officers assigned to a specialized unit can carry out the following acts:

- take part in electronic conversations under a pseudonym ;

- be in contact via electronic means with the individuals suspected of being offenders of the above-mentioned crimes ;

- extract, acquire and retain in this way evidence and data on individuals suspected of being offenders of the above-mentioned crimes.

In contrast, those acts cannot constitute an incitement to commit a crime, failing which they may be invalid (Articles 706-25-2, 706-35-1 and 706-47-3 of the Code of Criminal Procedure).

1.2 Remote data capture

The above-mentioned Law of 14 March 2011 allows investigators to remotely capture suspected individuals' data in real time.

Thus, when investigating organized crime, the Investigating Judge, after obtaining the opinion of the public prosecutor, can allow the investigators to place a technical device in order to access data in all places and to record, store and transfer these data without the consent of the individuals concerned (Article 706-102-1 of the Code of Criminal Procedure).

Those technical devices may be placed on site or remotely on a computer or a mobile phone for instance.

They may not be used for any other aims than researching and finding criminal infringements actually investigated by the Investigating Judge. However, if these operations reveal other criminal infringements, this cannot constitute a ground for the nullity of incidental proceedings (Article 706-102-4 of the Code of Criminal Procedure).

2. THE SEARCH FOR DIGITAL EVIDENCE

The search for digital evidence can be achieved by two means: computer searches (2.1) and computer requisitions (2.2).

2.1 Computer searches

The seizure of any electronic data necessary for the discovery of the truth is carried out by placing in the hands of justice, either the physical medium holding this data or a copy of the data made in the presence of those persons present at the seizure (Articles 56 al. 5 and 97 al. 3 of the Code of Criminal Procedure).

If a copy is made, then on the orders of the district prosecutor, any electronic data the possession or use of which is illegal or dangerous to the safety of persons or property may be permanently erased from any physical medium that has not been placed in judicial safekeeping (Articles 56 al. 6 and 97 al. 4 of the Code of Criminal Procedure).

Judges have first acknowledged the possibility to only seize electronic data in order to cause the least possible disruption to the seized individual's economic activity (e.g., Crim. 14/11/2001: Bull crim. 2001, no 238). The legislator enshrined this possibility in the Law of 21 June 2004. However, in practice this type of seizure is rare. Indeed, electronic data analysis can be time-consuming, which leads the Investigating Judge to seize the physical media for further analysis by specialized units.

2.2 Computer requisitions

A judicial police officer may order any person (establishment or organisation, whether public or private or any public services) likely to possess any documents relevant to the inquiry in progress,

including those produced from a registered computer or data processing system, to provide them with these documents. Without legitimate grounds, the duty of professional secrecy may not be given as a reason for non-compliance (Article 60-1 of the Code of Criminal Procedure).

Beyond this order to provide the investigators with a document in particular, public organisations or private legal persons who can intervene by means of telecommunications or computers, must make available information helpful for the discovery of the truth, at the request of a judicial police officer, where it is stored in one or more computer or data processing systems that they administer (Article 60-2 al. 1 of the Code of Criminal Procedure).

Finally, a judicial police officer, intervening on the orders of a district prosecutor authorised in advance by a (decree from the liberty and custody) judge, may require Internet service providers and Internet hosts to take without delay all appropriate measures to ensure the preservation, for a period that may not exceed one year, of the text of the information consulted by persons using the services provided by the operators. Those operators must make the required information available as quickly as possible by means of telecommunication or computers (Articles 60-2 al. 2 and 3 of the Code of Criminal Procedure).

* *
*

The legislator successfully adapted the legal framework regarding the search for evidence to new developments in criminality by increasing the use of computer science.

Nevertheless, this trend also causes difficulties.

Thus, for instance, legal privilege which is often threatened when searching for evidence may be even more at risk when using computer science as an investigative mean.

Indeed, it may be difficult for a person whose computer device has been seized to make sure that investigators have not disregarded legal privilege by, for instance, illegally consulting the content of emails exchanged between this person and his or her lawyer.