ARTICLE:

ELECTRONIC EVIDENCE IN SWISS CRIMINAL PROCEDURE

By **Bertrand Perrin, Marc Rémy** and **Romain Roubaty**

Dealing with cyber crime in Switzerland[1]

Notion of cyber crime

The terms "computer crime", "computer-related crime" and "cyber crime" comprise a wide variety of new phenomena, including new types of crime as well as traditional crime committed in connection with computer data and systems. The common denominator and characteristic features of all of these offences can be found in their relationship to computer systems or to computer networks. The major substantive aspect of this categorization is the relationship between crimes and computer-based data or the relationship to computer-based information.[2]

This paper examines electronic evidence in general. Legal theorists have dealt at length with the question of cyber crime, advancing various principles, particularly on the subject of collecting and using evidence. These principles are equally applicable, even if the computer system is not connected to a network. The developments set out below will apply, unless stated otherwise, to cyber crime is the broad sense, namely, to offences involving or which could involve the use of a computer, with or without a network connection.

Council of Europe Convention on Cybercrime

The Council of Europe adopted the Convention on Cybercrime on 23 November 2001.[3] The preamble of the Convention indicates that the main objective is to pursue a "common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation". Forty-seven States have already signed the Convention (at the date of writing), while sixteen countries still have to ratify it and set the date for its entry into force.

On 18 June 2010, the Federal Government approved a message proposing the ratification of this agreement by the Swiss Parliament,[4] and on 18 March 2011, the Parliament adopted the Convention.[5] It is the first international treaty on criminal offences committed via the internet and other computer networks, with particular reference to copyright, computer-related fraud, child pornography and network security. It also provides for a series of procedural powers, such as the search of computer networks and the interception of content data.

In 2008, the Federal Government expressed the opinion that Swiss legislation largely satisfied the requirements imposed by this Convention. Nevertheless, the government has mentioned the need to adapt the rules of the Penal Code (PC)[6] and the Law on International Mutual Assistance in Criminal Matters (IMAC)[7] to bring them into line with the Convention.[8] As for the Swiss Code of Criminal Procedure (CCP), which entered into effect on 1 January 2011, the Federal Government, in a press release of 18 June 2010, stated that no amendments were needed. According to the statement, the new text fulfilled the requirements of the Convention on Cybercrime.

In substantive law, the present Section 143*bis* PC ("wrongful access to a computer system") has been amended and supplemented. As it stands now, it punishes (upon an information being laid) anyone who, without right, obtains access to a computer system belonging to another which has been specially protected by the owner of the computer or an employee authorized to protect a computer or network. The offender must have acted "without intention of self-enrichment". This requirement, which has been

1 *For a general introduction to the legal position in Switzerland that pre-dates the changes outlined in this article, see Marc Schwitter 'Switzerland' in Stephen Mason, International Electronic Evidence (British Institute of International and Comparative Law, 2008).*

2 *Ulrich Sieber, General Report on Internet Crimes, XVIIIth International Congress of the International Academy of Comparative Law, Washington D.C. 2010, p. 8.*

3 *ETC (European Treaty Series) No 185.*

4 *Message concerning the Council of Europe Convention on Cybercrime, available at http://www.bj.admin.ch/bj/fr/home/themen/kriminalitaet/gesetzgebung/cybercrime__europarat.html.*

5 *The Federal Government has to ratify it. The Convention will probably enter into force for Switzerland on 1 January 2012.*

6 *RS (Recueil systématique du droit fédéral) 311.0.*

7 *RS 351.1.*

8 *Press release dated 28.02.2008, available at http://www.admin.ch/aktuell/00089/index.html?lang=fr&msg-id=17476.*

criticised by legal writers, has been abandoned. Moreover, a new paragraph 2 will sanction anyone who puts into circulation or renders accessible a password, a programme, or any other data which he knows or ought to know are to be used for the purpose of wrongfully gaining access to a computer system, within the meaning of the first paragraph. Thus the amendment contemplated by the Federal Government should permit the sanctioning of the illegal distribution of access codes or other similar data which, in criminal law, constitute acts in preparation of piracy. This new offence will be prosecuted by its own motion.

As stated above, the Federal Law on International Mutual Assistance in Criminal Matters has been amended to make it compatible with the Convention (new Article 18b IMAC). The fundamental change allows the competent Swiss authorities for mutual assistance in criminal matters to transmit computer traffic data[9] before the conclusion of the mutual assistance procedure. Authorisation to transfer such data in advance is justified, provided that there is a close link between the efficiency of the criminal prosecution and the speed with which the requested information is transferred. Nevertheless, this transmission to the foreign authority is subject to strict conditions, and is only permitted in two cases (article 18b(1)(a) and (b) IMAC):

a) the interim measures indicate that the source of the communication covered by the request is located abroad, or

b) this data is collected by the executing authority pursuant to an authorised real time surveillance order.

The new provision also provides that data transferred in this way cannot be used as evidence before the decision on the granting of assistance has become final (article 18b(2) IMAC). Otherwise, in the event of appeal, they could be excluded as evidence.

Swiss cyber crime authorities

Jurisdiction for the prosecution of cyber crime rests with the federal authorities (Federal Public Prosecutor), or the cantonal authorities (cantonal public prosecutors[10]).

The scope of federal jurisdiction is governed by sections 23 ("Federal jurisdiction") and 24 CCP ("Federal jurisdiction in relation to organised crime, the financing of terrorism and white-collar crime").

The judicial and police authorities of the cantons are primarily responsible for the criminal investigation of cyber crime in Switzerland. Computer crimes in the strict sense, that is those which by definition are committed with the aid of a computer, include misappropriation of data (section 143 PC), unauthorised access to a computer system (section 143*bis* PC), destruction of data (section 144*bis* PC), fraudulent use of a computer (section 147 PC), fraudulently obtaining a paying computer service offered to the general public (section 150(3) PC). However, ordinary offences committed with the aid of the internet or a computer, such as representations of violence (section 135 PC), fraud (section 146 PC), hard core pornography (section 197(3) and (3*bis*) PC) offences against personal honour (section 173 and following PC), racial discrimination (section 261*bis* PC), infringement of copyright (section 67 LDA) and violation of trade or manufacturing secrets (section 162 PC[11]) also fall within the scope of computer crime.

On the national level, the Swiss Coordination Unit for Cybercrime Control (CYCOS) is an entity that receives reports from people who discover suspect web sites and, where appropriate, forward the information to the Swiss or foreign law enforcement authorities. It also carries out its own research into illegal web site content. Finally, this service monitors trends in internet crime and issues periodical reports on the subject.

Article 35 of the Council of Europe Convention on Cybercrime requires States to create points of contact that are available at all times.[12] These must facilitate national and international criminal investigations into cyber crime, particularly by acting as intermediaries between the domestic and foreign authorities responsible for these tasks. In Switzerland, the Federal Office of Police (Fedpol) is responsible for this mission. The Federal Office of Justice (FOJ) handles tasks relating to mutual assistance and extradition.

The Swiss Code of Criminal Procedure Rules

An historic change

The Swiss Code of Criminal Procedure entered into force

9 More specifically, it concerns the following data: sender, recipient, date, duration, size and itinerary of the communication.

10 On 1 January 2011, the position of investigating magistrate has ceased to exist in Switzerland. Conducting the preliminary inquiry and prosecuting offences in connection with the investigation rest exclusively with the Public Prosecutor.

11 Rules are available on the web site of the Swiss Coordination Unit for Cybercrime (CYCOS, Cybercrime Coordination Unit) at http://www.scoci.ch/cyco.php?language=en.

12 Message concerning the Council of Europe Convention on Cybercrime, p. 42.

on 1 January 2011. It is the culmination of a long process of unification of criminal procedure, which until recently was regulated by 26 cantonal statutes and by the Federal Law on Criminal Procedure (LCP) of 15 June 1934.[13] As of 1 January 2011, therefore, the substantive criminal law (Swiss Penal Code) and the criminal procedural rules (Swiss Code of Criminal Procedure) are unified at the federal level. In general, this development has been welcomed by practitioners, particularly by members of the judiciary, since crime knows no boundaries. Until now, the differences between the many cantonal criminal procedures have primarily benefited the very people that they were supposed to prosecute.

Collection and use of electronic evidence

Electronic evidence

Electronic evidence (also known as digital evidence) is any probative information in electronic form that can be used as evidence in court. Electronic information can be collected from the use of information material, the recording and analysis of network traffic (such as computer or telephone networks), or the examination of digital copies (image copies, file copies).[14]

Rules for electronic evidence do not differ from general rules of evidence. However, electronic evidence has specific characteristics.[15] First, it is often difficult to report. This is particularly the case when a cybernaut commits offences, but there is no trace left on his hard disk.[16] Secondly, electronic evidence can be altered during its collection and when it is analysed. It is therefore the responsibility of law enforcement authorities, including the police, to ensure that the evidence is preserved, and to document all stages of its collection (continuity of evidence), as illustrated by Julien Lhuillier and Anne-Sophie Peron-Verloove:

> "Not only can technological media be very unstable, it can also be quickly obsolete, and it is the responsibility of the people in charge of preserving technological evidence to pay attention to the maintenance conditions (optimum temperature, humidity and light conditions; safe from fire, flooding, infestations; away from any magnetic force that can wipe out electronic data from the evidence media); however they should also be concerned about being able to use this evidence despite the lapse of time."[17]

Personal conviction of the judge

Section 139(1) CCP stipulates that the criminal authorities shall "employ every type of admissible evidence which, based on the state of scientific knowledge and experience, can serve to establish the truth". Swiss law contains no absolute limits on the type of evidence that may be presented in court. Criminal authorities can therefore use new evidence resulting from scientific progress even if it does not expressly feature in procedural law.[18]

In Swiss law, the principle of the personal conviction of the judge (moral evidence system) is the corollary of the freedom of evidence principle. Every element that can prove a fact may be used. The judge assesses and weighs up all the evidence in order to arrive at a personal conviction. All evidence, even circumstantial, can sway his conviction. His decision is dictated by his conscience. He convicts or acquits according to whether or not he is convinced of the guilt of the accused.[19] However, his conviction must be arrived at reasonably and he must provide a reasoned judgment,[20] which allows a review by the appeal authority. As a rule for assessing evidence, the principle of 'when in doubt, in favour of the accused' implies that the judge cannot declare that he is convinced that the facts established are adverse to the accused when an objective assessment of all the evidence leaves serious and ineluctable doubts as to the existence of such facts.[21]

The judge must not render an arbitrary decision. A decision would be arbitrary if, when assessing the evidence and establishing the facts, the judge fails to take account, without a valid reason, of evidence that could alter the decision, if he is obviously mistaken about the meaning and scope of the evidence, or if, based on the evidence collected, his findings are untenable.[22]

Search (sections 241-248 CCP)

"Search" is an extensive search for evidence, assets or persons located in private premises, with or without the

13 *RS 312.0.*
14 *For a definition of electronic evidence, see Stephen Mason and Burkhard Schafer in Stephen Mason, general editor, Electronic Evidence, (2nd edn, LexisNexis Butterworths, 2010), 2.03.*
15 *For a discussion on the characteristics of digital evidence, see Stephen Mason and Burkhard Schafer in Electronic Evidence, Chapter 2.*
16 *Christiane Féral-Schuhl, Cyberdroit, Le droit à l' épreuve de l' Internet, (Dalloz-Sirey, Paris 2009), p. 906.*
17 *Julien Lhuillier and Anne-Sophie Peron-Verloove, "Cadre normatif et pratique de lutte contre la cybercriminalité en Suisse", in Lukas Heckendorn Urscheler and Annelot Peters, editors, Swiss Reports Presented at the XVIIIth International Congress of Comparative Law, Geneva, Zurich and Basel 2010, p. 315; note also the extensive discussion of this topic in Electronic Evidence, Chapters 1, 2, 3 and 4.*
18 *Message concerning the unification of criminal procedure law, p. 1161.*
19 *Gérard Piquerez, Traité de droit pénal suisse, 2e édition, Geneva, Zurich and Basel 2006, Nos. 708-709, pp. 448-449.*
20 *Gérard Piquerez, Traité de droit pénal suisse, 2e édition, Geneva, Zurich and Basel 2006, No. 710, pp. 450-451.*
21 *See for example the judgment of the Federal Tribunal (ATF) 127 I 38, 40-41 consid. 2a.*
22 *See for example ATF 129 I 8, 9 consid. 2.1.*

consent of the beneficial owner. It can be aimed, in particular, at documents (hard copies) and recordings (for instance electronic storage) in order to determine whether, in the interests of the inquiry, their seizure would be justified. Under the Swiss Code of Criminal Procedure, it rests with the Public Prosecutor to order searches. However, in situations where there is danger in delay, the police are also competent to order a search (section 241(3) CCP).

Wherever possible, a backup copy should be made directly after searching computer equipment. It is advisable to protect against any preinstalled programme on the machine that can be activated remotely to wipe out data.[23]

Before the search takes place, the holder of the documents can offer an explanation about the contents of the documents and recordings that are to the subject of the search. He can also object to the search, for example by stating that the recordings are covered by professional confidentiality or by establishing his personal relations with the accused. In such a case, the Public Prosecutor or the police must follow the procedure known as "placing under seal" (section 248 CCP).[24] This procedure prohibits the Public Prosecutor from examining and using the documents and recordings placed under seal, and grants him 20 days in which to apply to the court for an order to remove the seals. The court must rule on the matter within one month. Its decision is final.

The placing under seal needs some explanation. Although many electronic storage media do not pose any particular problems for this procedure, there are others which cause a few technical concerns. These can involve outdated as well as more avant-gardist technology. For instance, where the device is powered off, this does not appear to be problematic. However, if the investigating authorities were dealing with a PDA which does not use flash memory,[25] and only has RAM,[26] for example running under Windows Mobile 2003, by leaving the device unplugged there is a significant risk of irremediable loss of data. When the device is switched on, the data that the investigating authority wants to analyse will probably have disappeared. If the device is plugged in, it could become even more problematic. If, for analysis reasons, the device needs to be kept switched on (problem of access code or RAM capture), either a plug has to be taken out of the packet under seal in order to maintain the power connection and ensure that the plug remains correctly in place, or an investigation has to be conducted in situ, which can create difficulties in terms of the competency of the personnel, equipment or time.[27] Unfortunately, these problems can build up. If the device remains switched on, measures must be taken to ensure that the data stored on it cannot be deleted or reset remotely. This would require placing the object under seal in a Faraday cage, a practice which is not necessarily well known or mastered by all the participants involved in a search, and which requires the proper equipment.

From the legal point of view, the provisions on search in the CCP will satisfy article 19(1) and (3) of the Council of Europe Convention on Cybercrime, which requires States to provide measures to enable authorities to search and seize recorded computer data and data storage media.[28]

In the case of international mutual assistance in criminal matters, the issue may be whether a foreign request, for example to save traffic or content data, can be executed rapidly. This question is relevant for anyone who is familiar with the slow pace of certain procedures. Under the current statutory provisions, the Swiss authority requested by a foreign authority to rapidly execute, for example, a search for documents, can act by means of interim measures (article 18 IMAC). However, the foreign authority, within a period set by the Swiss authority, must file a formal request for assistance, thereby confirming and completing the request for interim measures.

An alternative to search: obligation to deposit (section 265 CCP, "Obligation to hand over items and assets")

In accordance with the proportionality principle, coercive measures using force will only be employed if the investigating authority cannot obtain the object in any other way. For this reason, the CCP provides for the person under investigation to voluntarily deposit the object at the behest of the authority. However, this possibility is only granted in cases where there is no risk that a warning of the measure will cause it to fail (where the person under investigation may collude with others or might conceal the objects). In practice, it involves an order being served on the presumed holder to deposit a document or a recording within a given time, on pain of a criminal sanction for failing to comply with a decision of the investigating authority, or a disciplinary fine (section 265(3) CCP).

23 Julien Lhuillier, Anne-Sophie Peron-Verloove, p. 315.
24 In practice, the documents or recordings are placed in an envelope under seal or in a sealed container.
25 Memory with the properties of live memory, but with no disappearance of data in the event of power loss.
26 Standard live memory. The content is lost when it is no longer connected to the mains.
27 For an extensive discussion on this topic, see Electronic Evidence, Chapter 3.
28 Message concerning the Council of Europe Convention on Cybercrime, p. 25.

The obligation to deposit does not apply to the accused who cannot be compelled to actively implicate himself, or to persons who have the right to refuse to deposit or give evidence (section 265(2)(a) and (b) CCP). This provision applies to a third party who has information that is useful to the inquiry. In the computing field, an example of this would be an obligation order for eBay to deposit hard copies and computer-data storage media that would enable the identification of a thief who used the platform to steal from his victims.

The obligation to deposit in section 265 CCP is compatible with article 18 of the Council of Europe Convention on Cybercrime, which stipulates that the investigating authority must be able to compel anyone to submit stored computer data in his possession or control.[29] The question of seizure will now be considered.

Seizure (sections 263-268 CCP)

Search is very often accompanied by a subsequent measure – seizure – which is the "temporary withdrawal of the right to make use or to dispose of a thing".[30] Seizure does automatically follow on from a search, since the documents and recordings can be spontaneously handed over to the investigators. Under the provisions of the CCP, it rests with the Public Prosecutor to order seizures, subject to situations of danger in delay. In the latter cases, the police or even individuals also have this power (section 263(3) CCP). In the case of individuals, it is only a provisional measure, in the sense that the Public Prosecutor must formally order the seizure.

The seizure can cover various objects, particularly evidence and objects that are likely to be confiscated (section 263(1)(a) and (d) CCP). In the computer field, any electronic information that can be used as proof in a judicial matter will be qualified as evidence. The investigators will, in particular, examine information media and network traffic. Objects that must be confiscated are notably those that have been used to commit offences. Thus, the computer of a specialist in internet fraud can be seized, both as evidence and as an object that must be confiscated (a tool used in the offence). As in the case of a search, an objection to seizure triggers the procedure of "placing under seal". This subject is covered in the section on search.

The Council of Europe Convention on Cybercrime also suggests another type of seizure – the obligation imposed on a third party to preserve data. Swiss law partly meets this requirement to the extent that article 15(3) of the Law on Postal Service and Telecommunications Surveillance (LSCPT)[31] imposes on Internet Service Providers (ISPs) the obligation to preserve traffic and billing data for a period of six months. Only ISPs are subject to this obligation.

Real time collection of traffic data (sections 269-281 CCP)

Swiss law authorises the law enforcement authorities to collect traffic, billing and content data in real time. Traffic and billing data can be solicited in cases involving crimes or misdemeanours pursuant to section 273 CCP, while content data can only be solicited in connection with the offences mentioned in section 269 CCP (particularly serious offences). Article 21 of the Council of Europe Convention on Cybercrime requires States to adopt measures to allow the collection of content data "in relation to a range of serious offences to be determined by domestic law". Consequently, the Convention does not require Switzerland to expand or reduce the list of offences in which the law enforcement authorities are permitted to use such a surveillance measure.

Recommendations of the International Organization on Computer Evidence (IOCE) on the Collection and Use of Electronic Evidence

According to the information on its web site, the International Organization on Computer Evidence (IOCE) is an international forum that enables law enforcement agencies to exchange information and knowledge concerning computer investigation and digital forensic issues. To ensure the reliability of digital evidence, the IOCE encourages States to respect certain general principles. It is interesting to note that while these principles do not constitute legal rules, they allow, from a technical point of view, the positive realisation of precautions that should be taken during computer related investigations. These principles are as follows:

1. All of the general forensic and procedural principles

29 *Message concerning the Council of Europe Convention on Cybercrime, p. 24.*
30 *Message concerning the unification of criminal procedure law, p. 1227.*
31 *RS 780.1.*

must be applied.

2. Upon seizing digital evidence, actions taken should not change that evidence (integrity).

3. When it is necessary for a person to obtain access to digital evidence, that person should be trained for the purpose.

4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.

5. An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

These recommendations are very useful, but they cannot and can never be applied to the letter.[32] It is possible to spend a great deal of time focusing on and defending form over substance. Good investigation practices can change rapidly and, in certain circumstances, by applying them too rigidly, essential evidence can be lost. For example, in cases where the justice system investigates encrypted containers,[33] the most efficient way to obtain the data is to copy them when their volumes have mounted (that is when the volumes are installed for use by the encrypting software) and they are therefore readable. This requires intervention on the incriminated machine and, inevitably, the electronic evidence will be modified by the investigator. Obviously, the investigator must make a report of what he does and to comply with the spirit of the relevant recommendations. In theory, therefore, everything will be in order, but in realty it does not necessarily follow that all the technical details are sufficiently clear for most law officers. It will then be easy to confuse the issue and to try to cast doubt on the quality of the investigation by relying on known and published rules, which are not understood in detail.

Conclusion

Investigations in the computer world have specific characteristics with regard to collecting and using evidence. Even though these measures are based on ordinary provisions of the Code of Criminal Procedure, "technical" guidelines must also be observed, particularly to prevent the evidence from being modified during collection.

According to the Federal Government's conclusions, the Swiss legal provisions comply with the requirements of the Council of Europe Convention of Cybercrime. The Swiss Parliament has made a few amendments to the Penal Code and the Federal Law on International Mutual Aid in Criminal Matters (section 143*bis* PC and section 18b IMAC). On the organisational level, the Federal Administration (Fedpol/FJO) will also need to increase the numbers of people employed to a certain extent.

The next step would be to prepare a treaty on the international level, drawing inspiration notably from the United Nations Convention against Corruption. Cyber crime is too much of a global threat to be tackled on the regional level. The present process of ratification of the Council of Europe Convention represents a step in the right direction. However, a legal text is only of value if it is applied effectively, and with the necessary means, by all those who are responsible for its implementation.

Bertrand Perrin, Doctor of Laws, attorney at law, MA Economics, is Professor of law at the Institut de lutte contre la criminalité économique, ILCE (Neuchâtel) (Institute of Economic Crime Investigation (IECI)) and Deputy Cantonal Judge (Lausanne).

http://www.ilce.ch

Marc Rémy is a Prosecutor in Neuchâtel.

Romain Roubaty is a mathematician and Professor of Computer Science at the Institut de lutte contre la criminalité économique, Managing Director of RoubaTIC Sàrl (computer forensics).

32 For a list of other recommendations respecting the handling of digital evidence, see the list in Appendix 1 to Electronic Evidence.

33 An encrypted container is a virtual volume which exists in the form of an encrypted file and can be read by appropriate software.