Electronic evidence in cybercrime cases and the CTOSE project

Leroux, Olivier; Pérez Asinari, María Veroníca; Dinant, Jean-Marc

Published in:
World Internet Law Report

Publication date:
2003

Document Version
Publisher's PDF, also known as Version of record

Electronic Evidence in Cybercrime Cases and The CTOSE Project

By Jean-Marc Dinant, Olivier Leroux and María Verónica Perez Asinari

Introduction

The CTOSE[1] project (Cyber Tools Online Search for Evidence) is a European project, funded by the European Commission (in the frame of the Information Society Technologies "IST" Program) that was set up in December 2001. It is supported by a consortium, headed by the JRC (Joint Research Centre) and consists of a five-way partnership consisting of three universities (Namur, Stuttgart and St. Andrews) and two private bodies (Alcatel and Qinetiq). The main purpose of the project is to encourage wider use of electronic evidence in cases of disputed electronic transactions (communications) without jeopardising security and privacy requirements. CTOSE aims to ensure that electronic traces which are collected as evidence, will be admissible before a court, comprehensible to those called upon to make judgments about the transactions concerned, and sufficiently *reliable* and well-authenticated to be accepted as proof of an electronic event.

Although computers and digital evidence have existed for more than 60 years, the age of computers on workers' desks, computers at home, and computers in the hands of criminals is a far more recent phenomenon. Electronic evidence, once the province of classic "computer crime" cases like hacking and intrusion, is now to be found in every category of crime – from harassment to homicide, from drug dealing to security fraud. Computers and digital media are nowadays increasingly used in unlawful activities and investigation of any criminal activity may produce electronic evidence. The rapid growth in the number of criminal cases involving electronic evidence however, has frequently found the judiciary and law enforcement bodies ill-prepared to deal with the new issues created as a result.

The CTOSE project must try and bridge the gap between the level of current knowledge of electronic evidence and the extent of the knowledge needed to successfully deal with electronic evidence.

In this context, the *Centre de Recherches Informatique et Droit* ("CRID")[2] recently organised a conference in order to present some of the results of the CTOSE project and to further discuss certain key issues.

The Conference aimed at exploring three questions, namely:

- under what circumstances can electronic traces be considered as admissible evidence?
- to what extent can electronic evidence be considered technically accurate?
- how far can the processing of traces carried out without compliance with personal data protection legislation undermine the validity of electronic evidence?

In order to address these questions, the legal and technical aspects related to the processing of e-evidence and personal data protection were considered from different perspectives: the CTOSE project; the current state of play under European law; legitimacy and practice; and the point of view of different interested parties.

Aspects of Procedural Law

With regard to the handling of electronic evidence, some questions arise related to the legality of the evidence on the one hand, and the weight of the evidence that has been collected on the other. These are addressed below:

Admissibility of Evidence

The admissibility of evidence is a matter for the judge to decide. He or she must only take into account probative elements that have been lawfully acknowledged as admissible for the purpose of the dispute. As the rules determining conditions under which pieces of evidence have to be declared admissible or not depend, to a great extent on the underlying fundamental principles of evidence in respective countries and have been largely designed by case law, the way the admissibility of evidence will be assessed differs from one country to another. Still, any piece of evidence that has been gathered in violation of these rules will be inadmissible and the judge will have to exclude it from the trial. The handling of electronic evidence (*i.e.*, the way it is captured, analysed, stored, managed, and presented for investigation) has to be compliant with E.U., international and national legislation to be admissible in the context of a dispute. Furthermore, the nullity of a piece of evidence could imply the nullity of the whole subsequent proceedings which are based upon the evidence – in some cases rendering an entire trial null and void. Issues relating to the admissibility of the evidence are therefore, to be distinguished from questions related to the relevance of proof, because the most relevant evidence is potentially more prejudicial for the whole judicial process than no evidence at all.

In principle, continental law countries (and many others) operate according to the principle of free introduction and free evaluation of evidence (*système de l'intime conviction*). Since there are no strict legal rules concerning the admissibility of evidence in these systems of law, the judge is in principle, allowed to use all kinds of evidence. Every means of proof is permitted in principle, as long as it was gathered according to specific rules and respecting general principles of law. In

this system, the judge decides whether the offence exists or not and has complete freedom to consider the relevance of the evidence gathered. In such legal systems, electronic evidence derived from computer records is admissible in principle.

However, this "liberty" does not mean that the evidence is admissible in any given case. The liberty of proof in criminal cases knows some limitations that have been decided mainly on the case law.

First, the gathering of pieces of evidence cannot attempt to fundamental human values. Secondly, pieces of evidence must be obtained in a lawful way. Thirdly, no violation of the general principles of law can occur in that process. Pieces of evidence gained in violation of privacy rules, breach of professional secrecy, or of the secrecy of correspondence, illegal wiretapping and others menaces, could then lead to their inadmissibility.

Views differ on the desirability of admitting evidence which has been obtained illegally (for example by a crime, tort or breach of contract, or in contravention of statutory or other provisions governing the powers and duties of the police in investigating crimes). The same controversial question arises when the evidence has been collected improperly (for example by trickery, deception, threats or inducements).

At one extreme, the view is taken that evidence which is relevant should not be excluded because of the means by which it was obtained. To exclude it would, in some cases, result in injustice including the acquittal of the guilty party. If this opinion is favoured, all evidence which is necessary to enable justice to be done should be admitted. At the other extreme, however, one can think that illegally or improperly obtained evidence should always be excluded; to admit it might encourage the obtaining of evidence by such means. Following this opinion, all such evidence should be excluded, even if it sometimes results in injustice.

Laws of evidence, which vary largely from one country to another, represent in many countries a compromise between those two extreme views. And problems may occur when procedural provisions provide specific regulations for the proof of judicial acts, or proof of legal documents.

Weight of the Evidence

The notion of "weight of the evidence" refers to the relevance of the probative elements brought before a court. This consists of assessing the pertinence of proof, or of any element supposed to prove any fact. The relevance (the weight of the evidence) is a matter for appreciation by the judge. Evidence is relevant if it is logically probative or disapprobative of some matter that requires proof, or makes the matter which requires proof more or less probable. Relevance is a question of degree determined by common sense and experience.

Having considered the legal principles related to the weight of the evidence, what are the factual issues arising in the digital world?

Collecting E-Traces

By default, an increasing amount of Internet servers routinely collect traffic information about their users. When an incident occurs, it may be reported to the system administrator ("sysadmin"), notably by a complaint from a legitimate user, the dysfunction of the computer system itself, or by an alarm triggered by an Intrusion Detection System (IDS).

In certain cases, relevant e-traces are retained for investigation purposes. This is only the case however, where the head of a company is clearly committed to such a policy – usually where a company has suffered severe damage, or if it appears that the offence has originated from inside the company. Often, the investigation has to lead to a particular individual before it is admissible in court.

Judges are seldom computer experts and very often they employ an expert witness to give technical advice. Typically, such an expert will be asked to examine the e-traces, to produce copies and to determine if they are reliable and if they do indeed prove what the plaintiff has alleged. It is also common to ask an expert witness to determine the amount of direct damages if a suspect has been arrested and pleads not guilty. Just like a judge, the technical expert will have to be convinced about what has been done, by who, at what time and whether it was done with or without malicious intent.

In many cases, the system administrator (who is often unaware of the benefits of retaining e-evidence) will simply restore the functioning of the information system as soon as it is possible to do so. Very often, the simplest way of repairing the system is to restore the original data from a previous backup. To be quite sure that the operating system itself has not been corrupted, there is a temptation to restore a full image of a backup disk, created in a non-suspect period, from scratch. The Internet server may also be easily restored within a few minutes. Unfortunately, by doing this, the sysadmin may erase all clues to understanding the incident, and, ultimately the possibility of identifying and prosecuting the author if it appears to be a criminal offence. The CTOSE Methodology teaches that the first thing to do after an incident is to freeze the electronic traces left behind.

Furthermore, malicious hackers wanting to erase their own traces may tend to issue an obvious attack (typically a web defacement) just for the purpose of pushing the sysadmin to reboot the system and revert to the earlier version of the data. In so doing, the sysadmin may, as a consequence, replace the most recent log files containing e-traces of offences by a former version that does not contain any substantive intelligence about the offence. For this reason, the CTOSE Methodology recommends that all log files be retained on a separate, dedicated write-only computer

Investigating the Incident

This point is actually the easiest to demonstrate. It is not usual for a company to deliberately commit an attack against it's own IT infrastructure. At the same time, it is common for the plaintiff's lawyers to dramatically

overestimate the damage. As far as human paranoia is concerned, following a cyber attack, many employees falsely believe that everything going wrong with their IT networks is a direct consequence of the attack. The computer experts will have to examine the e-traces collected and estimate if the damages alleged are linked to the incident reported. If this is the case, they may estimate, the amount of the direct damage caused, drawing on recent cases as a comparison. The experts are in an ideal position to provide an impartial description of the damages directly linked to the incident. For instance, in the concrete case of a simple web defacement, a Judicial expert will examine not only the number of visitors of the defaced web pages but also their origin, as appearing through the IP address of the visitors. If internal company employees are the only ones to have seen the defaced web pages, it is then very difficult to claim any damage resulting from a bad commercial reputation.

In contrast to what happens in the actual world, a criminal offence in cyber world does not imply the physical presence of the criminal on the scene of the crime. There are no fingerprints or genetic traces, no camera and no direct testimony – simply, in the most easily solvable cases, an identifying number on a file. The identifier could be one of many things and with the notable exception of electronic signature, it has to be noted that identifiers commonly used as identifications means will seldom be accepted as proof of authentication, as they are easily forged by an intruder. For instance, the IP address in the case of a DoS using UTP and not TCP (typically against a DNS server) may not be considered secure. All the routers are not parameterised in such a way that they impend the transmission of illegal IP addresses form outside an ISP network. In fact the ISP has no concrete interest in doing this. The Mac ADDRESS itself can commonly be changed by configuring the Ethernet Card Driver. A password may have been guessed or spied, *etc.*

Furthermore, this kind of identifier may lead to a particular computer[3] (a physical terminal) but it does not confirm who was behind the keyboard at a given moment (as far as it is possible to know the exact date and time of the attack.

Establishing the Presence of Mala Fide

Even if the suspected person has no alibi, or if it can be proved that he or she was working from the computer terminal concerned at the time of the offence, there are many cases where the person present in front of the keyboard is not the conscious author of an incident. The most common case exists in a virus attack. Many viruses send a copy of themselves to the recipients stored in the address book of the mailing program – without leaving any traces on the computer itself. It is also very common for hackers to use multiple IP-relays in various countries to attack a remote target. In this particular case, the IP relay may be found on the suspected computer. But, even if this IP masquerade program is found on the terminal, it does not prove that this program has actually been used to commit the attack. It is relatively straightforward to put an automatic and invisible hyperlink into a classic web page, forcing the browser of every visitor to the page to commit a severe attack against, for example, the official website of the Secret Services!

It is clear that the firm conviction of the expert will also be funded on the profile of the suspected person and more precisely on the technical knowledge that this person has or does not have.

The Protection of Privacy and Personal Data in the Handling of E-Evidence

Coming back to admissibility issues, and as pointed out above, the handling of e-evidence must be compliant with E.U., international and national legislation to be admissible in the context of a dispute (*principe de la régularité des preuves*).

Apart from procedural law requirements (applicable as well in offline as in online worlds), special attention has to be paid to the privacy and data protection legal framework. We start from the premise that enormous amounts of Internet users' personal data are collected on the Internet by different parties and through different mechanisms. Sometimes a user is aware of this and has consented to it, other times the data is collected unlawfully, *i.e.*, without an individual's agreement or their knowledge.[4]

If a dispute arises, this data could be considered as electronic evidence. For this evidence to be admissible it has to have been obtained (and processed) lawfully. That means that the part of this data that can be considered as "personal data"[5] has to be processed (before, during and after the disputed event) in compliance with the applicable legislation protecting it, at national, international and supranational level.

By default, many HTTP servers generate a logbook containing the traces of actions performed by every web visitor. The logbook is a key instrument, which will normally be used as electronic evidence during a dispute. However, system administrators should consider the rights[6] and obligations[7] emanating from Directive 95/46/EC. Even if they are not normally able to identify directly who the user behind an external IP address, revealed in the log file is, they can identify the Internet Access Provider who has given it by checking in the appropriate Whois registry: RIPE, ARIN or APNIC, *etc.* By knowing the Internet Access Provider it is then potentially possible to connect the IP address – recorded on the system administrator log file – to the name and other data of the user/client of the IAP (the user has signed a contract with the IAP where he provides his name, address, and other personal data and the IAP usually "log" the date, time, duration and dynamic IP address given to the Internet user in a log file). Here, we have to remember Recital 26 of Directive 95/46/EC, and the reference to "*means likely reasonable*" to be used either by the controller or *by any other person* to identify the said person" [emphasis added].

The procedure described for identification does not seem unreasonable, excessively costly or difficult. In this case, the identification would not be done by the

controller (the person who has collected the IP address, a website administrator, for instance) but by a third person (the Internet Access Provider). Normally, a warrant issued by a judge will be necessary to make a legal connection.

In these cases there is no doubt about the fact that one can talk about personal data in the sense of the Directive.[8] Notwithstanding, this data will be "personal data" as far as the Internet Access Provider stores the log files through which it is possible to make this identification. As soon as these log files are deleted, the IP addresses stored in the log files of the web administrators become "anonymous data", and Directive 95/46/EC is no longer applicable.

So, considering that electronic evidence can contain personal data, it becomes necessary to comply with Directive 95/46/EC, and identify the risks for violation of privacy and personal data protection rules. Basically, the CTOSE Project has identified three major risks: civil liability, criminal liability, and inadmissibility of electronic evidence.

Concerning civil liability, it is important to bear in mind that every person has the right to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the processing in question. Article 23 of Directive 95/46/EC states that:

> "1. (...) any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the Directive is entitled to receive compensation from the controller for the damage suffered.
>
> 2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage".

In terms of criminal liability, the punishment of infringements to the national laws transposing the Directive will vary in different Member States, since this area of law is not harmonised within the European Union (procedural law, criminal law, *etc.*). However, the Directive rules that

> "Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive".[9]

Many European personal data protection laws penalise the violation of data protection principles with fines or imprisonment.

Finally, applying the principles explained above, it is reasonable to conclude that there is a risk of inadmissibility of the electronic evidence that has been collected in violation to privacy and data protection rules. So, any exception to the rights and obligations described by the Directive (national laws transposing it) and also by the European Convention on Human Rights and Fundamental Freedoms (Article 8) can only be operated strictly following the requisites described therein.

Conclusion

The gathering of e-evidence will suppose both a strong computing knowledge as well as legal awareness to collect evidence with respect to legal requirements. Neglecting both aspects may lead to non-admissibility of evidence before a court and potentially ruin hundreds of hours of work by specialised forensic experts. Considering that there is no harmonisation in procedural law at the E.U. level, it will be left to national statutes and case law to determine the rules of admissibility and weight of electronic evidence.

Electronic traces automatically stored in log files will, in a huge majority of cases, be considered as referring to personal data. Infringements of data protection rules could indeed be considered as an offence, polluting the evidence gained by the way of this violation and can thereby often lead to the inadmissibility of the evidence.

When electronic traces are considered as admissible evidence, their electronic character does not raise a problem in itself, but their weight will be assessed regarding the circumstances under which the collection has been made. Even if electronic traces are often considered unreliable proof because of their technical characteristics (they can be easily changed and even forged from scratch), they can often appear more reliable than corporeal pieces of evidence because of their size and their intrinsic coherence. Computer systems routinely record lots of data (much more than corporeal supports can offer) and, provided these data are not altered, they could prove more reliable than human supports (such as testimonies). On balance, it appears that electronic traces are not as unreliable as they might appear in comparison with other means of proof.

1 This paper is a resume of what has been presented by the authors at the Conference "Collecting and Producing Electronic Evidence in Cybercrime Cases", which was held in conjunction with the CTOSE project, on May 8–9, 2003 at the University of Namur, Belgium. All presentations from the Conference are available at: *www.ctose.org/info/events/workshop-8-9-may-2003.html*

2 *www.droit.fundp.ac.be/crid/*

3 This is an optimistic hypothesis – in many cases the identifier may lead to no computer at all. Consider for instance, a fixed IP address that has not been used before or a Mac-Address in a DHCP log file that may not be the address of an Ethernet Card.

4 In the SMEs sector specifically, even the data controller (system administrator) may be unaware about the fact that he or she is collecting personal data, since log files are created by default.

5 Personal data is defined by Article 2(a) of Directive 95/46/EC as "any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". This definition has to be understood jointly with Recital 26 of the same Directive: "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; (...)".

6 The rights of the "data subject" are identified in Articles 10, 11 (information), and 12 (access, rectification, erasure, or blocking) of Directive 95/46/EC.

7 The obligations of "data controllers" are identified in Articles 6 (respect of data quality principles), 7 (respect of legitimacy of processing), 18 (notification to the national data protection

authority), 17 (security and organisational measures), etc., of Directive 95/46/EC.

8 It has to be noted that the concept of personal data has been transposed into U.K. law in a more restrictive way than the one of the Directive. This is not the case in most of other E.U. Member States. See, for instance: Opinion issued by the Belgian Data Protection Authority *"Avis d'iniciative concernant la compatibilité de la recherché d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les telecommunications"*, Numéro de rôle 44/2001. See also: G. RUE and F. DE PATOUL "L'affaire Napster ou le difficile équilibre entre le droit d'auteur et le respect de la vie privée", *Revue Ubiquité, Dr. tech. Info.*, FUNDP, DGTIC, CRID, N° 12, Juin 2002, Belgium.

9 Article 24 of Directive 95/46/EC.

Jean-Marc Dinant is a computer scientist and works as a researcher at the Centre de Recherches Informatique et Droit ("CRID") in Namur, Belgium. He is also an Expert Witness on the Belgium High Court Circuit. María Verónica Perez Asinari is a lawyer and also works as a researcher at the CRID. Olivier Leroux is is a lawyer and also works as a researcher at the CRID.