ARTICLE:

REMOTE FORENSICS AND CLOUD COMPUTING: AN ITALIAN AND EUROPEAN LEGAL OVERVIEW

By **Dr Giuseppe Vaciago**

Although it has become clear that computer forensics – the practical analysis of digital data following the acquisition of a bit-stream image of a suspect's hard disk – suffered a setback with the wide adoption of mobile devices and the increasing use of flash memory and encryption systems, it is undoubtedly also the case that it experienced a fundamental change due to the incredible expansion of cloud computing systems. In this article, the aim is to study the jurisdictional problems that cloud computing systems cause and the possible solutions at an EU level that have been adopted by legislators and the courts of the European Union in relation to the gathering of digital evidence that may be concealed in the 'clouds'.

Introduction

There has been heated debate on both sides of the Atlantic in recent years on the wisdom of empowering law enforcement authorities to use remote forensics technology to obtain access to the digital data storage devices (laptops, servers, smart telephones, etc) of suspects.

Law enforcement agencies find it increasingly difficult to locate the servers on which incriminating data are stored, since the perpetrators tend to rely on remote access connections to store and process data using faraway devices.[1] The increasing popularity of cloud computing,[2] moreover, has made conventional crime detection even more difficult: the very strengths of cloud computing, which allows anyone anywhere in the world to use publicly accessible software to process data stored in a virtual cyberspace location, could be put to devious use by criminals to store incriminating data on a server located beyond the jurisdiction of the courts of their country of residence, preferably in a State with no judicial cooperation treaty with that country.

Over the last few years, various approaches have been offered to solve the 'loss of location' of digital evidence in the 'cloud world'. The traditional approach is the territorial principle by virtue of which the court in the place where the data is located has jurisdiction. This approach essentially prohibits any type of investigation, because even the cloud provider might not know exactly where the data is located. Another approach is the nationality principle by virtue of which the nationality of the perpetrator is the factor used to establish criminal jurisdiction. This principle imposes certain restrictions, since the perpetrators in a cyber crime case might easily be foreign nationals, given that cyber crime is generally transnational and there is no need for physical proximity. Furthermore, data does not have a nationality, because it is an attribute of an individual. A third approach is the 'flag principle', which basically states that crimes committed on ships, aircraft and spacecraft are subject to the jurisdiction of the flag State, regardless of their location at the time of the crime (article 22, Convention on Cybercrime[3]). Since digital data is

1 *Orin S. Kerr, 'Searches and Seizures in a digital world', Harvard Law Review, 119 (2006), 531.*

2 *Janna Quitney Anderson and Lee Rainie, The Future of cloud computing, (Pew Internet & American Life Project, 11 June 2010), available at http://pewinternet.org/Reports/2010/The-future-of-cloud-computing.aspx.*

3 *Article 22 of the Convention on Cybercrime (Jurisdiction): 1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: (a) in its territory; or (b) on board a ship flying the flag of that Party; or (c) on board an aircraft registered under the laws of that Party; or (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State [….].*

constantly changing, this principle also seems to be applicable to cloud computing. However, to apply this to the cloud computing scenario, it is necessary to remember that this principle could motivate cyber criminals to select a cloud computing provider under a 'pirate flag'.

Finally, a recent discussion paper, prepared by the Council of Europe within the framework of the global Project on Cybercrime, suggested the 'Power of Disposal Approach'.[4] From a practical point of view, a regulation based on the power of disposal approach would make it feasible for law enforcement officers to obtain access to a suspect's data within the cloud. Law enforcement officers would only have to legally obtain the username and password combination and be able to prove that additional requirements have been met. This type of approach certainly overcomes any legal issue, but a balance must be struck with the legitimate need for privacy and the rights of the suspect.

Legislative measure of the Convention on Cybercrime

To overcome the obstacles generated by the 'data loss' location of digital evidence, signatory States have endowed their respective judicial authority and law enforcement agencies with a number of legislative measures in the implementation of articles 18 (Production Orders), 19 (Search and Seizure of Stored Computer Data) and 20 (Real-time Collection of Traffic Data), of the Convention on Cybercrime.

Under article 18 of the Convention on Cybercrime, signatory States are required to empower their respective judicial authorities to issue Production Orders requiring any person or party (obviously, including ISPs) to submit to law enforcement authorities specific digital data in the possession or control of the person or party in question, and stored on a computer system or data storage medium.[5]

Some Italian commentators hold the view that Production Orders could also be issued to compel the disclosure of data pertaining to web users based outside the boundaries of a signatory State, provided that the users have entered into a contract for services provided by an ISP that operates, amongst other things, in the signatory State in question.[6] This interesting approach appears, however, to conflict with the principle of sovereignty, and may, in any event, be applied solely to subscriber information (article 18(1)(b) of the Convention on Cybercrime), since only ISPs located within the territory of the signatory State in which the Production Order is issued may be compelled to submit user-generated content (article 18(1)(a) of the Convention on Cybercrime).[7]

Pursuant to article 19 of the Convention on Cybercrime, moreover, signatory States are required to ensure that, upon discovering that pertinent digital evidence is, in fact, stored on another server, their respective law enforcement agencies are also empowered to search the other server, provided, however, that the latter is located within their national borders, and that the digital data to be seized may be accessed from the server initially covered by the related search and seizure warrant.

In any event, even when searching for specific data stored on a computer system located within the borders of the signatory State in which the Production Order is issued, law enforcement agencies may encounter serious difficulties as a result of the sheer volume of data to be parsed to find useful digital evidence. In light of these obstacles, the Convention on Cybercrime requires law enforcement agencies to be empowered to compel the IT manager to provide 'as is reasonable' the information necessary for successfully securing the digital evidence sought.[8]

4 *Jan Spoenle, Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?, (31 August 2010, Council of Europe Project on Cybercrime), available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf.*

5 *Dr Marco Gercke, Understanding Cybercrime: A Guide For Developing Countries, (April 2009), 192, available at http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html.*

6 *Dott Fabio Licata, 'La Convenzione del Consiglio d'Europa sul cybercrime e le forme della cooperazione giudiziaria: una risposta globale alle nuove sfide della criminalità transnazionale' (The Cybercrime Convention of Council of Europe and Cooperation between Law Enforcement Authorities), in a workshop of Consiglio Superiore della Magistratura, held in Rome on 19 September 2005, at 17, available (in Italian) at http://appinter.csm.it/incontri/relaz/12009.pdf.*

7 *On this issue, see point 170 of the Explanatory Report on the Convention on Cybercrime: 'Paragraph 1 of this article calls for Parties to enable their competent authorities to compel a person in its territory to provide specified stored computer data, or a service provider offering its services in the territory of the Party to submit subscriber information. The data in question are stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications. Instead of requiring States to apply systematically coercive measures in relation to third parties, such as search and seizure of data, it is essential that States have within their domestic law alternative investigative powers that provide a less intrusive means of obtaining information relevant to criminal investigations'.*

8 *A similar approach was adopted by the cyber crime experts who, in 2001, drew up a Model Law on Computer and Computer Related Crime, no. 202, for the implementation of the Convention on Cybercrime in Commonwealth countries (LLM(02)17, October 2002); see section 11 of the 'Model Law' available at http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.*

Finally, article 20 of the Convention on Cybercrime requires that law enforcement authorities of signatory States to be afforded real-time access to web traffic data, that is to say the electronic records of a suspect's on-line activities (web sites visited, e-mail correspondents, downloads, etc). Towards this end, signatory States must enact national legislation requiring ISPs either to provide law enforcement authorities with the software tools necessary for directly collecting and recording traffic data subject to search and seizure, or alternatively, to collect and record such data on an ad hoc basis, pursuant to a judicial or prosecutorial order to such effect.

As in the case of the evidentiary seizure of e-mail, 'Production Orders' and the 'Real-time Collection of Traffic Data' contemplated in articles 18 and 20 of the Convention on Cybercrime respectively are very similar to the interception of communications, which are subject to specific restrictions pursuant to article 8 of the European Convention on Human Rights.

Sadly, these three crucial 'crime-detecting' tools, entrenched in the Convention on Cybercrime, are available only in part to Italian law enforcement agencies. Whilst the Italian Code of Criminal Procedure does, in fact, currently contemplate procedural instruments designed to achieve the same results (the appointment of a digital evidence specialist to assist law enforcement officers pursuant to article 348, paragraph 4; discovery orders within the meaning of article 248; and interception of communications regulated under article 266-*bis*), in ratifying the Convention on Cybercrime, Italy failed to avail itself of a significant opportunity to fine-tune this set of 'crime-detecting tools'. As a matter of fact, at present, the majority of ISPs, without considering that the Convention on Cybercrime had suggested the adoption of 'software tools for directly collecting and recording traffic data subject', submit log files and IP addresses of suspects to law enforcement authorities without any validation of digital evidence of the transmission that could be achieved by adhering to best practices of digital forensics through the use of the hash function and an adequate time stamp.

Italian and German case law on remote forensics technology

Several European countries are currently considering legislation that would invest their law enforcement authorities with powers to remotely monitor and record the traffic data of suspects in real time to an extent that far exceeds the scope of the procedural tools outlined above,[9] whilst, on the other shore of the Atlantic, the FBI has already successfully tested a peculiar type of spyware (CIPAV) specifically designed for such a purpose.[10] In any event, it is amply clear that by allowing law enforcement officers to monitor the on-line activities of a blissfully unaware suspect from the air-conditioned comfort of their offices, remote forensic techniques have proven far more cost-efficient and effective than conventional detective work and, moreover, without any jurisdictional problems.

At the same time, it would be perilous to lose sight of the dangers that such invasive techniques might entail in terms of the suspect's fundamental rights and freedoms. Great care must, accordingly, be taken to properly weigh all the legal interests involved, and strike a delicate balance between the prevention of crime and public security, and the need to protect the suspect's due process, privacy and other human rights.

On this issue, it is interesting to note that the Supreme Court evinced no need to address the constitutionality of a prosecutorial warrant – issued pursuant to article 234 of the Italian Code of Criminal Procedure, authorizing the use of surreptitiously installed ghost software to obtain a copy of the digital data stored on a desktop used by the suspect and located in a public office – on the grounds that the related evidentiary seizure order did not pertain to a flow of communications but merely entailed the mining of data already stored on the suspect's desktop, that is to say, a 'a one-directional flow of data' contained within the computer's internal circuitry.[11]

The Supreme Court moreover held that, in the case in question, this technical activity was repeatable, given that 'copying the stored files neither altered the

9 *John Blau, 'Debate rages over German government spyware plan', 5 May 2007, in Computerworld Security, available at http://www.computerworld.com/s/article/print/9034459/Debate_rages_over_German_government_spyware_plan?taxonomyName=Security&taxonomyId=17.*

10 *For further information on the CIPAV project, see Kevin Poulsen, 'FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats', Wired, 18 July 2007, available at http://www.wired.com/politics/law/news/2007/07/fbi_spyware; and Kevin Poulsen, 'Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years', Wired, 16 April 2009, available at http://www.wired.com/threatlevel/2009/04/fbi-spyware-pro/.*

11 *Supreme Court of Cassation, 5th Criminal Section, decision no. 16556 of 14 October 2009.*

same nor entailed the destruction of the database which remained totally unchanged, and therefore accessible and open to consultation, subject to the same terms and conditions, even upon conclusion of evidence gathering operations'. According to the Supreme Court, the copying in question amounted to no more than a repeatable operation that could be undertaken without informing defence counsel, much less inviting the latter to attend the proceedings, since the same operation could be reproduced and repeated a second time if need be for procedural purposes, although such need did not arise.

During the Supreme Court proceedings, however, counsel for the defence argued that the warrant issued by the public prosecutor, whilst authorizing no more than the seizure of a copy of the digital data in question, effectively entailed the interception of computerized communications. The scope of the prosecutorial warrant, in fact, covered not only the files already stored in the suspect's computer system through to the date of the related search and seizure, but also to any and all data input into the system in the future. This factual situation was confirmed by the operating procedures followed in executing the prosecutorial warrant, which included the surreptitious installation of ghost software on the computer system in question, for the purpose of copying files already stored on the computer, and subsequently copying in real time any and all data processed using the computer system, before, finally, transmitting all the data that was copied back to law enforcement officers on a periodic basis. As a result, the computer system used by the suspect was effectively subjected to digital surveillance for over eight months.

The ruling deserves criticism from two standpoints: first, the Supreme Court does not appear to have considered the fact that the alleged repeatability of the copying and transmitting operations necessarily implies that no further data processing was carried out using the computer system in question following the original operations; second, in support of its refusal to apply the statutory provisions regulating the interception and recording of communications, the Supreme Court goes no further than to point out that the flow of communications copied by and transmitted to law enforcement authorities did not pertain to electronic correspondence between two private parties, but focused solely on a 'unilateral flow of communications'. Whilst this approach is certainly reasonable, there still seems to be a cloud of mystery shrouding both the Supreme Court's refusal to apply article 266-*bis* which regulates the interception of a 'flow of communications pertaining to computerized or electronic systems, or otherwise among several systems', and its apparent tolerance of highly invasive evidence gathering techniques that go so far as to entail the prolonged monitoring of a computer system without judicial oversight.

A totally different approach was taken by Germany. On 20 December 2006, article 5.2(11) of the Law on the Protection of the Constitution in North Rhine-Westphalia was amended[12] with the introduction of provisions on remote forensics instruments, both on-line and by obtaining access to information technology systems.

The issue first came to the attention of the general public and legal scholars in 2006 when a state prosecutor applied to the Federal Court of Justice of Germany (Bundesgerichtshof) to authorize a remote search of computers allegedly containing data useful to continuing investigations, by applying an analogy to the law governing search and seizure operations conducted on a physical premises. The court dismissed the motion, holding that clandestine remote searches of computers could not be deemed analogous to raids conducted on physical premises, but left open the possibility for new laws to be enacted endowing law enforcement authorities with specific search and seizure powers in respect of electronic data. It was this latter portion of the decision that led to the amendment of the Law on the Protection of the Constitution in North Rhine-Westphalia.

The new provisions reinforced the domestic secret service known as the 'Federal Office for the Protection of the Constitution' (Bundesamt für Verfassungsschutz) by authorizing the establishment of an agency with the specific task of gathering intelligence by obtaining covert access to computer systems and secretly monitoring on-line communications and web traffic.

Private computer systems could be covertly accessed either physically, using hardware (interception of communications and bugs) or

12 *Law on the Protection of the Constitution in North Rhine-Westphalia (Gesetz über den Verfassungsschutz in Nordrhein-Westfalen) as mended on 20 December 2006, articles 5.2(11), 7.1, 5.3, 5.1 and 13 (VSG); Wiebke Abel and Burkhard Schafer, ' The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822', (2009) 6:1 SCRIPTed 106, available at http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp.*

'remotely', thanks to software (key logger and sniffer programs) installed on the target system without the owner's knowledge, for instance, in the form of Trojans incorporated within or disguised as harmless content, by convincing the hapless owner to voluntarily upload the relevant spyware or disclose passwords through cleverly devised social engineering and phishing initiatives.[13] Under the amendment in question, the above remote forensics operations could be launched without a warrant or court order of any kind, and there was no specified limit on how long a particular computer system and on-line communication could be subjected to surveillance.

In consideration of all these elements, the German Constitutional Court[14] determined that the constitutionality of the amendment had to be assessed in light of three distinct fundamental rights enshrined in the country's Basic Law (Grundgesetz – GG): the privacy of correspondence:

> Artikel 10
>
> (1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
>
> (2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.
>
> Article 10
>
> (1) The privacy of correspondence, posts and telecommunications shall be inviolable.
>
> (2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature'.

The inviolability of the home:

> Artikel 13
>
> (1) Die Wohnung ist unverletzlich.
>
> (2) Durchsuchungen dürfen nur durch den Richter, bei Gefahr im Verzuge auch durch die in den Gesetzen vorgesehenen anderen Organe angeordnet und nur in der dort vorgeschriebenen Form durchgeführt werden.
> Article 13
>
> (1) The home is inviolable.
>
> (2) Searches may be authorized only by a judge or, when time is of the essence, by other authorities designated by the laws, and may be carried out only in the manner therein prescribed'.

and the 'right to informational self-determination'.[15]

With regard to the privacy of correspondence, the Constitutional Court held that this fundamental privilege extended to all types of telecommunications regardless of the means of transmission used (cable or broadcast, analogue or digital transmission), and the type of transmitted content (speech, picture, sound, or other data). However, the court went on to assert that constitutional protection did not extend to telecommunications data stored on computerized devices after the communications process had been

13 *Matthew Lewis, Biologger – A Biometric Keylogger, (IRM Research Paper, December 2008) presented at the Black Hat Conference, Amsterdam, 27-28 March 2008, available at http://www.blackhat.com/presentations/bh-europe-08/Lewis/Whitepaper/bh-eu-08-lewis-WP.pdf; Episode 621 on Internet TV Hak5 entitled MiTM Javascript Keylogger, Social Engineering Toolkit and more available at http://www.hak5.org/?s=keylogger&x=0&y=0. This approach may not be easy to take, because many devices (particularly mobile devices) are protected through the use of DRM; which, in addition to preventing the installation of unauthorized software, provide a level of security that would make it difficult to obtain access by way of Trojan horses or other malicious software.*

14 *It is interesting to note that during the proceedings on the constitutionality of the amendment, in addition to three technical experts from academia (Prof. Felix Freiling, Chair of Computer Science at the University of Mannheim, Prof. Andreas Pfitzmann, head of the privacy and security group at Dresden University of Technology and Prof. Ulrich Sieber, director at the Max Planck Institute for Foreign and International Criminal Law) the German Constitutional Court also heard a highly experienced hacker (Andreas Bogk, freelance hacker for Clozure, Inc., and CEO of Chaos Computer Club Events).*

15 *The right ' to informational self-determination' is derived from the combined provisions of article 2.1 and article 1.1 of the German Basic Law (Grundgesetz – GG) which enshrine the rights to ' free development of personality' and to ' human dignity' , respectively. The right to informational self-determination was established by the German Constitutional Court for the first time in a historic decision that led up to the passage of the German data protection law (decision of the Bundesverfassungsgericht of December 15, 1983, BVerG, paragraphs 65, 1, ‹···43···›; 84, 192).*

completed. In effect this means that it is not unlawful for the German secret service to surreptitiously copy data from the computer hard drives of suspects.

With regard to the second fundamental right engaged in the case, the Constitutional Court pointed out that the principle of the inviolability of the home, enshrined in article 13.1 of the Basic Law, only bars law enforcement officers from trespassing on private property in a bid to physically interfere with the hardware located on the premises. Since remote surveillance using Trojans or other spyware can be conducted regardless of where the target device may be located at any given time, location specific protection falls far short of ensuring adequate safeguards, especially since it is increasingly commonplace for computers to be operated outside or in transit between private premises.

Finally, the Constitutional Court examined the amendment in light of the 'right to informational self-determination' which protects web users against the collection and profiling of the data they post on-line. Once again, however, the remote forensics activities authorized under the amendment to the Law on the Protection of the Constitution go beyond the mere collection of personal data for profiling purposes, since clandestine access to just about any personal computer could, on its own, potentially prove a valuable discovery of highly sensitive data regarding its owner, without the need for any further profiling of the information collected in the process.

Having determined that the three fundamental rights enshrined in Germany's Basic Law afforded inadequate protection in the circumstances, the Constitutional Court opted to establish a new 'right to the confidentiality and integrity of information technology systems'. In the same way as the 'right to informational self-determination', this new 'right to the confidentiality and integrity of information technology systems' can be found in article 2.1 GG (right to the free development of one's personality), read in conjunction with article 1.1 GG (right to human dignity) and provides protection against State access to each and every information technology system taken as a whole, and therefore extends to all data, whether stored or transmitted.

Although the court conceded that the right to the confidentiality and integrity of information technology systems is not absolute and may be restricted in the interests of law enforcement and crime prevention, it took pains to point out that no encroachments on the newly created constitutional right could be tolerated, save to the extent necessary to safeguard even more imperative fundamental values which the court specifically limited to the life and liberty of other citizens, the foundational institutions of the State and the essential values of human dignity.

Conclusion

While declaring the amendment unconstitutional by reason of breach of the principles of proportionality and fair labelling, the German Constitutional Court has, however, left room for the passage of new laws authorizing remote forensic and on-line surveillance operations, albeit within the bounds of the principles outlined above.

It has, quite rightly, been pointed out that 'the digital citizen has, as a result of this case, come a step closer':[16] there can be no doubt that an increasing number of individuals not only use web technology on a daily basis, but actually 'live' on-line. The internet has become a place where people make friends, come together and exchange information and opinions. The German Constitutional Court acknowledged that the pre-existing legal framework was not robust enough to adequately protect 'digital' citizens against unwarranted State intrusion.

By the same token, the courts could well extend the same concept in the other direction in the future. At present, Trojans are considered mere software tools used by law enforcement officers to prevent, solve and thwart crime. What if, tomorrow, the courts were to consider Trojan fully fledged 'digital police officers' who inhabit cyberspace on an equal footing with 'digital citizens'?

Giuseppe Vaciago is a lawyer and has been a member of the Milan Bar since 2002. His PhD is in digital forensics, and he is a lecturer on IT Law at the University of Milan and Insubria University (Varese). He is also a visiting scholar at Fordham Law School (New York) and Stanford Law School.

http:// www.htlaw.it/en/

vaciago@htlaw.it

16 *Wiebke Abel and Burkhard Schafer, ' The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822'.*