Technologies and Business vs. Law - Cloud computing, transborder access and data retention: a legal perspective from the State which is conducting an investigation.

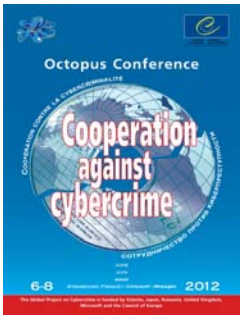
FRANCESCO CAJANI

Deputy Public Prosecutor, High Tech Crime Unit
Counter Terrorism Department
Court of Law in Milan (IT)

francesco.cajani@giustizia.it

Member of the Technical & Scientific Committee of IISFA
(International Information Systems Forensics Association) – Italy Chapter.

www.iisfa.eu



2012 Octopus Conference on Cooperation against Cybercrime
Workshop 4: Transborder access and jurisdiction
Council of Europe, Strasbourg, France

CONTENT

A) BACKGROUND

From October 2008 to March 2009, Eurojust and the Council of Europe asked me to prepare a concept paper for the First Strategic Meeting on Cybercrime in Athens and for the Octopus Conference in Strasbourg[1].

In the meantime, Google vs. Vividown trial took place in Milan: differently from the version given to the press by some Googlers, the real problem discussed in that case was the one regarding the application of European data protection rules in general[2] and, in particular, their impact on the web-business.

The last two years news, regarding the United Arab Emirates' and India' s perspective dealing with Blackberry interception problems, convince me to repropose my previous analisys, with some still topical considerations by the Law.

As written by a Judge in Italy, "*there is no endless prairie of the Internet where everything is permitted and nothing can be forbidden"*[3]. For this reason, also in the increasing topical issue of transborder access for investigative purposes, it is no longer possible to believe that everything is reduced to a *technology far west*, where Law succumbs to the technology.

---

[1] That paper has the title of "*Communication interception regarding Skype, Google, Microsoft & Yahoo! tools and electronic data retention on foreing servers: a legal perspective from the State which is conducting an investigation*".
See *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations /2079if09pres_cajani_investigation.pdf.*

[2] In an NYT article titled "*When American and European Ideas of Privacy Collide*" (*http://www.nytimes.com/2010/02/28/weekinreview/28liptak.html*), Adam Liptak wrote: *"On the Internet, the First Amendment is a local ordinance," said Fred H. Cate, a law professor at Indiana University. He was talking about last week's ruling from an Italian court that Google executives had violated Italian privacy law by allowing users to post a video on one of its services.*
In one sense, the ruling was a nice discussion starter about how much responsibility to place on services like Google for offensive content that they passively distribute.
But in a deeper sense, it called attention to the profound European commitment to privacy, one that threatens the American conception of free expression and could restrict the flow of information on the Internet to everyone.
"For many purposes, the European Union is today the effective sovereign of global privacy law," Jack Goldsmith and Tim Wu wrote in their book "Who Controls the Internet?" in 2006.
This may sound odd in America, where the First Amendment has pride of place in the Bill of Rights. In Europe, privacy comes first.
Article 8 of the European Convention on Human Rights says, "Everyone has the right to respect for his private and family life, his home and his correspondence." The First Amendment's distant cousin comes later, in Article 10".

[3] "*Non esiste … la sconfinata prateria di internet dove tutto è permesso e niente può essere vietato"* (page 95 of Judge Oscar Magi's sentence in the legal case Google vs. Vividown): see *http://speciali.espresso.repubblica.it//pdf/Motivazioni_sentenza_Google.pdf.*

B) THE OPPOSING START POINT

1. A space is not without law just because it is cyber

In cyberspace, the traditional country borders are cleared during the actions of the cyber criminal. The borders return later, when the detectives try to trace the actions of the criminal or terrorist, searching digital evidence possibly left by the author, and so useful for the investigation.

The main problem (it is even a cultural problem), is, as all detectives know, that cyberspace favours the suspects. Each time a cyber crime is reported across jurisdictions, it is necessary to ask the States affected to collaborate with the investigation, usually through a formal rogatory. Of greater importance, are the businesses providing electronic services with servers in another State, and whose servers and services the criminal act has used in some way. In theory, it is conceivable that a commercial entity will be nimble in responding to a legitimate request from another State to collaborate in tracking down a criminal. But this does not happen.

The commercial sector moves at a far slower pace than our counterparts across the world. Invariably, a barrier is immediately erected to any request with the excuse that they cannot help because it is not possible according to domestic law. This is what usually happens in relation to the electronic services provided by three of the most important internet businesses: Google, Yahoo! and Microsoft. The difficulty with intercepting the flow of communications in reasonably short time is a general problem, and it does not only apply to Skype[4].

2. "*No server no law*" opinion vs. "*no server but law*" opinion

We more often find ourselves dealing with opinions that differ. On the one side, there is the 'no server no law' view. Preference is given to the geographical location where the web servers are based: and often, the servers are outside the European Community. This is the case in respect of Google, Yahoo! and Microsoft.

This first point of view considers that national or European laws cannot be enforced because the web servers are in the United States of America. Of interest, regarding Skype, the servers could not be precisely identified (and therefore not intercepted), since they are organized as peer-to-peer nodes. On the other side,

---

[4] See Declan McCullagh, "*Skype: We can't comply with police wiretap requests*" (9 June 2008) available at *http://news.cnet.com/8301-13578_3-9963028-38.html?tag=bl.*

there is the opinion that I prefer, the 'no server but law' opinion. This view considers that the crucial point is the geographical location where the web services are offered, no matter where the web servers are, even for the purposes of law enforcement. As I usually say, *the server may be elsewhere, but the mouse is in Italy*.

3. Three scenarios

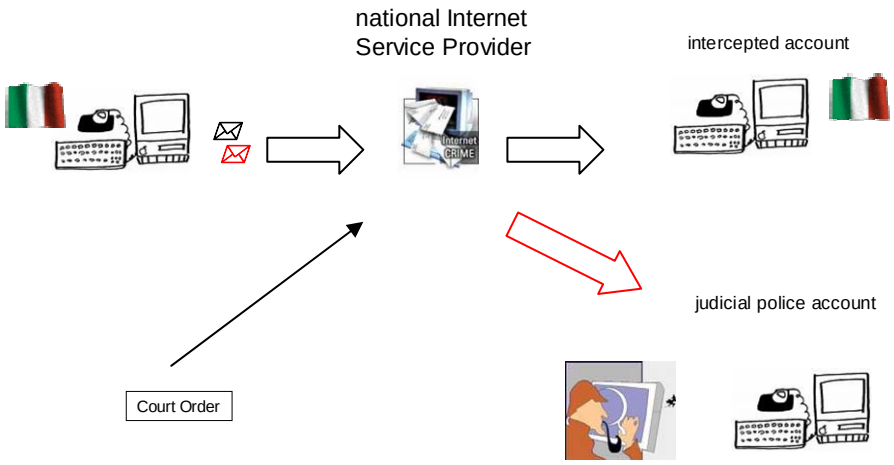
Essentially, there are three scenarios that affect the investigation of alleged crimes that include the use of networked communications. They can overlap, but the three that we need to consider can be divided into the availability of encrypted communication technology, the communication channel and communication data. Each are considered in turn below. The Italian Law regulates each scenario in a different way, and there are no reported decisions in relation to these matters at the time of writing. An important problem regarding each of these is also the length of time the data is retained.

3.1 The availability of encrypted communication technology

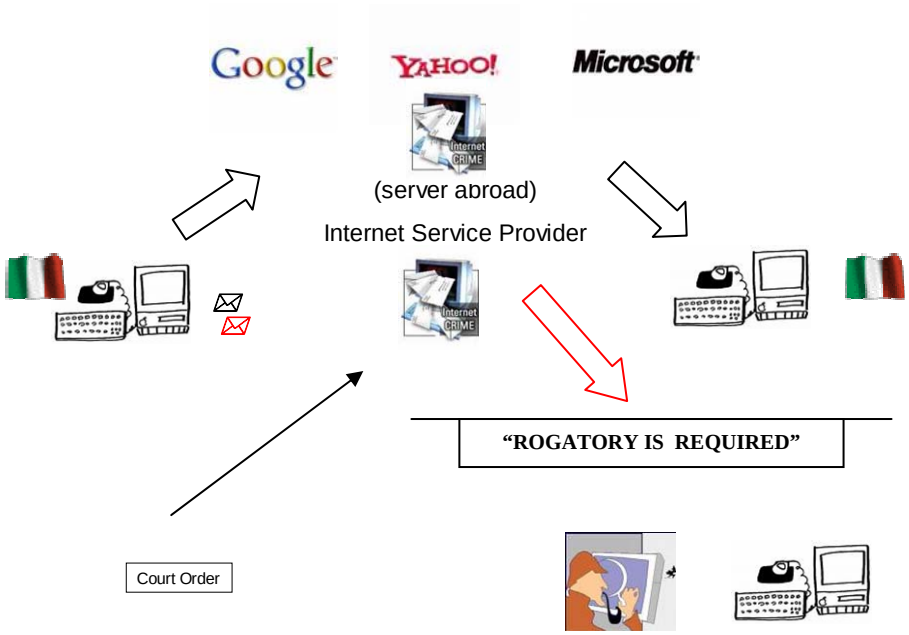
In the case of Skype and other Voice over Internet Protocol (VoIP) communications generally, the communication is encrypted. It is only possible to intercept a VoIP communication only when the investigating authority knows the exact location of the suspect's computer. The investigating authority will try to obtain access to the computer and install a program to enable interception to take place, and where it is not possible to reach the computer physically, social engineering techniques will be used to achieve the same aim. Naturally, it is only possible to undertake these actions with the authorization of a judge.

3.2 The availability of a communication channel

The vast flow of communications between people is now through e-mail systems. Often, the people under investigation are present in Italy, but they might use an e-mail system based abroad, such as Google or Microsoft: this occurs frequently, hence the reference to the 'no server no law' opinion. In fact it is not possible, in this case, to enforce an order issued by a judge by requesting that the e-mail accounts to be intercepted have the e-mail traffic redirected to the judicial police account. This might reduce costs and permit the interception to begin quickly, as it usually happens referring national societies with servers in Italy.



So the only possible mechanism is for the judicial police to notify the interception order to Google Italia or to Microsoft Italia (both with registered offices in Milan). However, their response is to indicate that the servers are in the United States of America, and they request a rogatory before they will implement the interception order. This is not good if the investigation concerns a murder or a kidnapping.



The situation is the same as with Skype – it is almost impossible to intercept communications. Only Yahoo! Italia (their registered office is in Milan) has an item of software called 'Yahoo! Account Management Tool'. This software allows e-mail to be intercepted, but it is of limited help.

3.3 The availability of communication data

This scenario refers to data relating to the use of the internet, such as log files. In the experience of some Italian investigation agencies, Microsoft Italia was the first to provide – without a rogatory but only with a request from the Italian Public Prosecutor – such data, not only referred to *@hotmail.it* e-mail, but including *@hotmail.com*.

At first, Google Italia considered it was necessary for a rogatory, but they changed their policy, and now provide all the data required if the request comes with an order from the Italian Public Prosecutor (not only from the Italian Judicial Police). Nevertheless, if an IP address (logged by the Google electronic systems with regard to an e-mail *@gmail.com*) is not related to an Italian or an European server, at the moment this society doesn't feel to be allowed to communicate it to the Italian Judicial Autority.

In comparison, Yahoo! Italia requests a rogatory, but only in some cases[5].

4. Some preliminary matters

In order to be better prepared to investigate alleged crimes, investigators have had to assemble lists of relevant information in relation to each Internet service provider (ISP), including: where the web servers are physically located; where the registered office of the ISP is located, and if the ISP has an operating branch in the State where the investigation is conducted. It is also necessary to know (in order to verify potential criminal liability) if the employees in the operating branches are in effective control of the local affairs of the ISP, or whether they are mere legal representatives.

[5] The rogatory is required if, at the time of the the creation of the electronic mailbox *@yahoo*, the user doesn't choose to be subjected to the Italian law. About the principle of the "Net Citizenship" see note 28.

5. Jurisdiction analysis as applied in the United States of America

If the '*no server no law*' opinion was accepted, it would be interesting to know what view an American judge would take. The scenario is: the ISP is an American company which also has a physical base in Europe and offers its services to European citizens; the ISP insists that their web servers are in one of the US states, for example in California, and as a result, the ISP is not subject to the laws of the UE State. The same could be argued in reverse. An Italian ISP uses the identical argument to a Federal court in the US, that is: '*sorry, but our servers are in Italy*'. Or, the same American company with servers in California summoned in a different U.S. Court (for example: Arizona).

I think a US judge will not accept such arguments, consider how the judges in the US analyse internet jurisdiction[6] having developed two general lines of analysis in determining whether jurisdiction can be exercised in cases involving internet activity. The first, a 'sliding scale' approach, seeks to classify the 'nature and quality' of the commercial activity, if any, that the defendant conducts over the internet.[7] The second analysis, called the 'effects test', seeks to determine to what extent a defendant's intentional conduct takes place outside the forum State.[8]

So, for a number of years, the U.S. state courts have been using an undisputed analysis, providing for U.S. jurisdiction, even if the web site is based on a server in another country. This means that a foreign internet entrepreneur, although lacking 'continuous and systematic' contacts with any U.S. forum state sufficient to subject him or her to general jurisdiction, may nonetheless be subject to personal jurisdiction in the U.S. based on two broad theories of 'specific' personal jurisdiction. Under the *Zippo* 'sliding scale' analysis, a U.S. court will classify the 'nature and quality' of any commercial activity that is conducted over the internet and place it on a continuum ranging from 'passive', where no business is conducted, to 'clearly conducting business'. The closer the internet activities are to 'clearly conducting business', the more likely that a U.S. court will exercise personal jurisdiction. Courts may also apply the *Calder* 'effects test' to determine whether the intentional conduct of the party was calculated to cause harm to the plaintiff within the forum state. Where a defendant 'purposefully directs' his activities towards the jurisdiction, he may be liable to legal action for any injury relating to or arising from those activities.

---

[6] G. J. H. Smith*, Internet law and regulation,* (Sweet and Maxwell, 3rd edition, 2002), pp. 347-349.
[7] *Zippo Manufacturing Co. v Zippo Dot Com, Inc*., 952 F. Supp. 1119 (W.D. Pa.1997).
[8] *Calder v Jones*, 465 U.S. 783 (1984).

C) THE UNITED ARAB EMIRATES' AND INDIA' S PERSPECTIVE

On March 2010, local media print and television reports said the United Arab Emirates' Communication and Information Technology Commission has asked Canada-based Research In Motion, the company that owns one of the most popular mobile device, to allow the telecommunications regulator access to monitor messages sent by BlackBerry Messenger, or BBM (a special messaging service for BlackBerry phone users).

As the BBC reported[9], the UAE's Telecommunications Regulatory Authority has taken issue with the encrypted networks used by Research in Motion, saying "*BlackBerry operates beyond the jurisdiction of national legislation, since it is the only device operating in the UAE that immediately exports its data offshore and is managed by a foreign, commercial organisation*".

It also said that misuse may have "*serious social, judicial and national security repercussions*".

BlackBerry phones went on sale before the country introduced its safety emergency and national security legislation in 2007.

"*RIM operates in more than 170 (one hundred and seventy) countries around the world and respects the regulatory requirements of governments*," said a company statement on March 2010. "*RIM is investigating the reported matter in the Kingdom of Saudi Arabia and will provide an update once further information is available to share.*"

But, on July 2010, another company statement said: "*Like many other countries, we have been working for a long time to resolve these critical issues, with the objective of finding a solution that operates within the boundaries of UAE law.*" Research in Motion told BBC News that they had no comment to make "*at this point in time*".

In August 2010, as the NYT reported[10], the Indian Ministry of home affairs, which is responsible for internal security, said Research In Motion had made "*certain proposals for lawful access by law enforcement agencies and these would be operationalized immediately*." He also said that "*The feasibility of the solutions offered would be assessed thereafter*."

I wondered why they had found a solution in such a short time…..

As the NYT noted, Research In Motion has more than a million BlackBerry users in India, one of its fastest growing markets.

---

[9] *http://www.bbc.co.uk/news/technology-10761210.*
[10] *http://www.nytimes.com/2010/08/31/technology/31rim.html?_r=2.*

According to the NYT, Indian officials did not provide details, but the telecommunications department "*would study the feasibility of all such services being provided through a server located only in India.*"

Skype and Google, which also uses powerful encryption technology for its Gmail email service, are expected to be among the next wave of societies to come under New Delhi's power.

"*If a company is providing telecom services in India then all communications must be available to Indian security services*," a spokesman for the Indian home Ministry told Agence France-Presse[11]. "*If Google or Skype have a component that is not accessible, that will not be possible*," he said. "*The message is the same for everybody*."

D) THE U.S. PERSPECTIVE

According to an article dated 2010 of the NYT.com[12], Federal law enforcement and national security officials were preparing to seek new regulations for the Internet, arguing that their ability to wiretap criminal and terrorism suspects is "going dark" as people increasingly communicate online instead of by telephone[13].

Essentially, officials want Congress to require all services that enable communications — including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct "peer to peer" messaging like Skype — to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages.

According to the NYT, to solve such problems, officials are analysing several of the proposal's requirements:

- Communications services that encrypt messages must have a way to unscramble them.

---

[11] *http://www.globaltimes.cn/business/world/2010-09/568980.html.*
[12] *http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=all.*
[13] "*In the United States, phone and broadband networks are already required to have interception capabilities, under a 1994 law called the Communications Assistance to Law Enforcement Act. It aimed to ensure that government surveillance abilities would remain intact during the evolution from a copper-wire phone system to digital networks and cellphones. Often, investigators can intercept communications at a switch operated by the network company. But sometimes — like when the target uses a service that encrypts messages between his computer and its servers — they must instead serve the order on a service provider to get unscrambled versions. Like phone companies, communication service providers are subject to wiretap orders. But the 1994 law does not apply to them. While some maintain interception capacities, others wait until they are served with orders to try to develop them. […] Moreover, some services encrypt messages between users, so that even the provider cannot unscramble them*".

- Foreign-based providers that do business inside the United States must install a domestic office capable of performing intercepts.
- Developers of software that enables peer-to-peer communication must redesign their service to allow interception.

Whatever is the real position of this American law proposal, all that I have read on the NYT is really very interesting.

We, poor Italians, have been working like crazy for years just because Google, Microsoft and Yahoo! servers were based in U.S.[14]. Finally even U.S. discovered that they haven't all the communication servers in their territories.

Thanks to technology and cloud computing services, the problem has become global.

And so it's really necessary to find sharing solutions.

What can we count on?

I don't think I can or I want to count on the business power…I prefer the power of Law, that is to suggest the reasonableness in respecting rules that benefit everyone and are already existing in Europe.

E) THE EUROPEAN PERSPECTIVE

In 2008 and 2009 papers of mine, the important question – regarding *a legal perspective from a UE State which is conducting an investigation* - was: "*which obligations and national laws can we expect observance of?*"

I quoted again three real important ones in the Italian experience, according to our EU laws.

6.1 The electronic communication rules

In Italy, the provisions of Decreto legislativo 1° agosto 2003, n. 259, Codice delle comunicazioni elettroniche[15] (Legislative Decree of 1st August 2003, n. 259 **electronic communication rules**) are fundamental. These rules have their origin in four EC Directives.[16] An important step has been taken by the Italian Ministero dello

[14] Or, at least, they let us believe it…. we've never seen them!
[15] Pubblicato sulla Gazzetta Ufficiale n. 214 del 15 settembre 2003.
[16] Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), OJ L 108, 24.4.2002, p. 7; Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), OJ L 108, 24.4.2002, p. 21; Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a

Sviluppo Economico (Ministry of Economic Development and Telecommunication), in that it has recently provided a written opinion[17] according to which Skype connections must be included in the electronic communication rules and are therefore subject to the general authorization provided by the law.

Consequently this involves the observance of the rules about the compulsory services required by the judicial authority and, in particular, to enable a legal interception to take place by competent national authorities, as also set out in article 6 of EC Directive 2002/20/EC, the Authorisation Directive:

> *Article 6*
> *Conditions attached to the general authorisation and to the rights of use for radio frequencies and for numbers, and specific obligations*
> *1. The general authorisation for the provision of electronic communications networks or services and the rights of use for radio frequencies and rights of use for numbers may be subject only to the conditions listed respectively in parts A, B and C of the Annex. Such conditions shall be objectively justified in relation to the network or service concerned, non-discriminatory, proportionate and transparent*

The relevant condition listed in the Annex is item 11:

> *A. Conditions which may be attached to a general authorisation*
> *[…]*
> *11. Enabling of legal interception by competent national authorities in conformity with Directive 97/66/EC and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

The combination of article 6 and paragraph 11 of the Annex could mean: if, for instance, in the future Skype decides to open a branch in Italy, this will be sufficient market conditions to enable Italian investigating authorities to require Skype to intercept communications if ordered so to do.

Moreover, according to these American societies, there are some U.S. laws that will prevent themselves from imparting anyone data regarding communications of their users.

---

common regulatory framework for electronic communications networks and services ("the Framework Directive"), OJ L 108, 24.4.2002, p. 33; Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), OJ L 108, 24.4.2002, p. 51.

[17] Note of 12 September 2008, following a specific request of the Direzione Nazionale Antimafia.

But **if the Italian Judicial Authority (and in this case not the Public Prosecutor but even the Judge who authorizes the wiretap) is able to testify that the communications are involving two Italian people (even if they are using an e-mail system *@.com)* both on the national territory[18], what kind of legal obstacle would it be? And this kind of denial doesn't sound as an act contrasting with the sovereignty of the applying State?**

6.2 The data retention rules

Secondly, we could expect the observance of the **data retention rules** (Decreto legislativo 30 maggio 2008, n. 109 – Legislative Decree of 30 May 2008, n. 109).[19] The provisions of articles 3 and 6 of Directive 2006/24/EC are relevant, and provide as follows:

> *Article 3*
> *Obligation to retain data*
> *1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communication network within their jurisdiction in the process of supplying the communications services concerned.*
> *2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.*
>
> *Article 6*
> *Periods of retention*

[18] In order to reference to the **traditional territorial and active personality principles of general criminal jurisdiction** see paragraph 7.
[19] Based on Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13/04/2006 P. 0054 – 0063.

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Data retention is an important matter in the investigation regarding cybercrime, as already shown in the EU Forum on Cybercrime Discussion Paper for Expert's Meeting on Retention of Traffic Data (6 November 2001):

To investigate and prosecute crimes involving the use of the communications networks, including the Internet, law enforcement authorities frequently use traffic data when they are stored by service providers for billing purposes. As the price charged for a communication is becoming less and less dependent on distance and destination, and service providers move towards flat rate billing, there will no longer be any need to store traffic data for billing purposes. Law enforcement authorities fear that this will reduce potential material for criminal investigations and therefore advocate that service providers keep certain traffic data for at least a minimum period of time so that these data may be used for law enforcement purposes.

Five years later, the same topics are in the initial points of Directive 2006/24/EC**:**

(9) …. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive […].

(10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.

(11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive […].

(18) In this context, Article 24 of Directive 95/46/EC imposes an obligation on Member States to lay down sanctions for infringements of the provisions adopted pursuant to that Directive […].

Seen these preconditions, the data retention rules are the true "test bench" in order to verify the real will, by any web societes, to actually cooperate with the European Authorities and Judicial Police to reach an efficacious contrast actions towards internet crimes.

It is clearly the opinion of Peter Schaar, President of the Article 29 Data Protection Working Party, that any EU rules can be applied to the organizations that turn their attention to provide services to European citizens:

> *'Although Google's headquarters are based in the United States, Google is under legal obligation to comply with European laws, in particular privacy laws, as Google's service are provided to European citizens and it maintains data processing activities in Europe, especially the processing of personal data that takes place at its European centre'*[20]

It therefore follows that the obligations of data retention also apply to Google, Yahoo! and Microsoft.

6.3 The COE Convention on Cybercrime rules

Finally, it is to be observed that the United States of America ratified the **Council of Europe Convention on Cybercrime** (Budapest, 23.XI.2001) on 29 September 2006, which provides for two precise obligations of **real-time** cooperation in articles 33 and 34:

> ***Article 33 – Mutual assistance regarding the real-time collection of traffic data***
>
> *1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.*
>
> *2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.*

[20] Letter from Peter Schaar to Peter Fleischer dated 16 May 2007, D(2007) 6016, available at *http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_google_16_05_07_en.pdf*

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Therefore, when a State such as Italy ratifies the Convention,[21] specific duties arise. As the ancient Romans said, and as the rules of international law remind us: agreements must be kept (*pacta sunt servanda*).

7. THE TRANSBORDER ACCESS LEGAL PROBLEMS

7.1 The sovereignty of the investigative action or the principle of the violated freedom?

Keeping into consideration what we have explained so far, I really believe that it's possible to point out a legal perspective inside the debated topic of the transborder access[22], even in the absence of specific provisions on the subject (as it is now happening for the Italian law).

And in fact, in many cases, it seems to be an apparent problem to focus the attention on the fact that the data to be investigated are abroad. That's not only following the "*no server but law*" thesis but also considering in such a particular hypothesis that we need to go over settings, almost like a dogma, the sovereignty of the investigative action (able to have a transnational effectiveness).

We need instead to reflect on the fact that, **in every legal system, the fundamental rights and freedom of individuals define the limits of the interest of a specific state towards the investigative activity.**

And therefore, as a legal principle to consider, it appears to be more suitable the one defined as "violated or compressed freedom".

Such a principle starts from the irrefutable statement that the fundamental rights and freedom are guaranteed among the borders of each state, according to the national law principles. And then we will need to take into consideration the place

[21] The Convention was signed by Italy on 23 November 2001, ratified on 5 June 2008, in force on 1 October 2008; Legge 18 marzo 2008, n. 48 Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno (Pubblicato sulla Gazzetta Ufficiale 4 aprile 2008, n. 80; s.o. n. 79) (Law of 18 March 2008, n. 48).

[22] See the Discussion papers on *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/.*

where such rights and freedom may be possibly violated or compressed through the investigative action of a state.

7.2 The three concrete and significant hypothesis in the investigative experience

The setting that we share as a starting point has to take into consideration three concrete and different hypothesis regarding the investigative experience.

A) INTERCEPTION OF ELECTRONIC COMMUNICATION FLOWS BY E-MAIL

This is the already mentioned case about the possibility to get an interception of e-mail communications even without the co-operation of the ISP, where the Judicial Police have acquired the e-mail authenticating credentials in another way (e.g. phone tapping). We are now facing a maximum constriction hypothesis of the fundamental rights and just for this reason the legal orders[23] usually plan as a rule the requirement of a Court order (and not of the Prosecutor).

But there are other cases where the investigative action compresses the fundamental rights of minor rank and therefore an order of the Prosecutor is enough.

B) ACQUISITION OF

1. DATA EXTERNAL TO THE COMMUNICATION (log files)

2. E-MAIL AND/OR OTHER DOCUMENTS LYING ON A SERVER

Only in the latter case, as we will see, we can speak of a potential access without the co-operation of the ISP, where the Judicial Police have acquired in another way (e.g. phone tapping) the authenticating credentials to a certain repository (e.g. e-mail box, data storage service such as dropbox, etc…)

7.2.1 INTERCEPTION OF FLOWS OF ELECTRONIC COMMUNICATION BY E-MAIL

In supporting the predominance of the "*no server but law*" principle, we have previously stated (par.61) that, if the Italian Judicial Authority is able to testify that the communications are involving two Italian people (even if they are using an e-

[23] In Italy is possible that a Public Prosecutor asks a Judge for an interception (phone or electronic communications tapping) only for serious crimes.

mail system *@.com)* both on the national territory, there wouldn't be problems of jurisdiction, even if the data of that communication pass through (and then technically don't reside in a static manner) abroad even for a certain path.

In these cases **there is no need to wonder which server the data resides on because here – according to the law – it points out instead the place where the freedom of communication is compressed, or rather the place where there is the person under interception** (which therefore matches with the place where the service is provided).

This approach is endorsed by the 2000 Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal matters between the Member States of the European Union.

In fact this Convention provides (TITLE III, art. 17 – 22) some rules which, according to the Explanation report[24], are also applied to the interception of communications which happened on the Internet.

We analyze Article 18, which regulates the situation where a state wishes to intercept a person located within its territory, but where there isn't the gateway accessible (because it is in another State). This is the most similar case to what we are discussing (i.e., I want to intercept a person who uses a box *@.com* on my territory, even if such a communication passes through a gateway in another State): we have an operation called "*interception from a distance*", that the 2000 Convention admits without any particular formalities (through the intermediary of a designated service provider present on the territory of the state that is conducting the interception)!

> ***Article 18 - Requests for interception of telecommunications***
>
> *1. Member States shall ensure that systems of telecommunications services operated via a gateway on their territory, which for the lawful interception of the communications of a subject present in another Member State are not directly accessible on the territory of the latter, may be made directly accessible for the lawful interception by that Member State* ***through the intermediary of a designated service provider present on its territory.***
> *2. In the case referred to in paragraph 1, the competent authorities of a Member State shall be entitled, for the purposes of a criminal investigation and in accordance with applicable national law and provided that the* ***subject of the interception is present in that Member State****, to carry out the interception through the intermediary of a designated service provider present on its territory without involving the Member State on whose territory the gateway is located.*

[24] *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:379:0007:0029:EN:PDF.*

This is also in line with the recalled art. 34 of the Cybercrime Convention, issued the following year.

A different mechanism is instead foreseen by art. 20 of the 2000 Convention, which rules the case in which a State wishes to intercept a person who is in the territory of another State, but it can also do this without requiring technical support in this state.

Only in this case it's foreseen the obligation to inform the other State, which instead will be able to oppose and even deny the continuation of these operations, since only in this case there is indeed a problem of jurisdiction.

But this information commitment, however, occurs only when you know for sure that the place where the person under interception is different from the one of the state which intercepts. And then, where such a place is not known, the State that is conducting the investigation (and also the interception) should not be involved in any legal obligation.

> ***Article 20 - Interception of telecommunications without the technical assistance of another Member State***
>
> *[...]*
>
> *2. Where for the purpose of a criminal investigation, the interception of telecommunications is authorised by the competent authority of one Member State (the "intercepting Member State"), and the telecommunication address of the subject specified in the interception order is being used on the territory of another Member State (the "notified Member State") from which no technical assistance is needed to carry out the interception,* ***the intercepting Member State shall inform the notified Member State of the interception****:*
>
> *3. The information to be notified by the intercepting Member State shall include: [...]*
>
> *4. [...]*
>
> *(a) Upon receipt of the information provided under paragraph 3 the competent authority of the notified Member State shall, without delay, and at the latest within 96 hours, reply to the intercepting Member State, with a view to:*
> *(i)* ***allowing the interception to be carried out or to be continued****. The notified Member State may make its consent subject to any conditions which would have to be observed in a similar national case;*

(ii) ***requiring the interception not to be carried out or to be terminated*** *where the interception would not be permissible pursuant to the national law of the notified Member State, or for the reasons specified in Article 2 of the European Mutual Assistance Convention. Where the notified Member State imposes such a requirement, it shall give reasons for its decision in writing; […]*

From such a Convention then we have a further proof of the fact that, **even new topics, like those of the transborder access, can be solved with the enforcement of the traditional principle of International Law** (the territory).

7.2.2 EXTERNAL COMMUNICATION DATA CAPTURE (LOG FILES)

It is evident that it is a different hypothesis from the interception also from the reference to the various European set of rules, like for example the Council framework decision 2008/978/JHA of 18 December 2008 on the European evidence warrant (EEW) for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, which expressly distinguishes the two cases:

Article 4 - Scope of the EEW

[…]

2. The EEW shall not be issued for the purpose of requiring the executing authority to:

[…]

(c) obtain information in real time such as through the ***interception of communications****, covert surveillance or monitoring of bank accounts;*

(e) obtain ***communications data retained by providers*** *of a publicly available electronic communications service or a public communications network.*

The investigative experience teaches that, in some cases, it's always necessary the co-operation with the ISP. But here, for the reasons above mentioned, there wouldn't be a problem of jurisdiction (as they are requests regarding citizens acting in the territory or having the nationality of the State which is conducting the investigation) but anyway, where these issues are adduced raised in a case[25], the latest principles of International Law such as those specified in art. 33 of the

[25] Actually, as we have seen in par.3.3, U.S. companies no longer require the rogatory letter to provide the log files.

Convention on Cybercrime ratify the obligation of co-operation among the states in real time and without any formality.

And more over the "*no server but law*" thesis is herewith taken into consideration because, as already mentioned at par. 6.2, unlike U.S. there is in Europe a specific legislation imposing a data retention *for periods of not less than six months and not more than two years.*

7.2.2.1 The Yahoo!, Google and Microsoft data retention period

The present situation, regarding the Italian experience, consists in Microsoft[26], Google and Yahoo![27] data retention periods not in line with the EC Directive, because it gives back informations about its e-mail boxes only about the last 30/60 days.

Anyone has a basic experience in cybercrime investigations can understand how short these periods are and how this situation effectively creates enormous damages to the investigations in progress in the European Communities States.

In my opinion, it could be different: we are in presence of societies which must be included in the provisions of article 3 of Directive 2002/58/EC:[28]

> *Article 3*
> *Services concerned*
> *1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.*

It is for such reasons, and independently from where the servers are physically located, they are required to comply with the obligations of the Italian and EU data retention rules… pace the American law! Really, the American laws don't provide for these societies determined data retention obligations so that the current adopted solutions appear to depend only on economical reasons.

---

[26] Microsoft has recently announced that it will hold data on European servers, allowing storage for a period of one year, being more in line with the forecast of the European directive/guideline about data retention.

[27] In 2007, the Public Prosecutor's Office in Milan had some difficulty with Yahoo! Italia around the 'Net Citizenship' concept. That is: when an Italian user registers an account from the webpage www.yahoo.it, he can choose which law his e-mail correspondence will be subject to. There is an item of software called Yahoo! Account Management Tool, which is used by all the Yahoo! branches. It returns the communications stored in e-mail boxes (*@yahoo.it* and *@yahoo.com* or both), but only in respect of those users that agree that Italian law applies: see paper quoted in note 1.

[28] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

For example, there was a great clamor in the media about Google's latest data-retention policy, which says that the company erases the last octet of a user's IP address from its server logs after nine months, and that it removes cookie data after 18 months. This policy was announced in the fall of 2008, and it was implemented before November 2009. But Google only agreed to such a scrubbing after years of pressure from governments and privacy advocates, and the European Union data protection authorities still say that the policy does not comply with EU law. Also the Court of Law in Milan said so in the Google vs. Vividown case[29].

On May 2010 the Article 29 Data Protection Working Party — an independent advisory body on data protection and privacy — sent public letters to the three major search engines[30] saying that although it welcomes their efforts to bring their data retention policies in line with the law, they haven't gone far enough.

"*Deleting the last octet of the IP-addresses is insufficient to guarantee adequate anonymisation*," reads the Working Party's letter to **Google.** "*Such a partial deletion does not prevent identifiability of data subjects. In addition to this, you state you retain cookies for a period of 18 months. This would allow for the correlation of individual search queries for a considerable length of time. It also appears to allow for easy retrieval of IP-addresses, every time a user makes a new query within those 18 months*."

In January 2010, **Microsoft** said that it plans to remove IP addresses entirely after six months, but that it will retain cookie data for a Google-like 18 months. It expects to implement this policy sometime next year. But again, WP29 wants cookies deleted after six months to ensure this sort of thing doesn't happen. "*The policy to delete IP addresses completely after 6 months is a significant improvement*", WP29 told Microsoft. "*However, in order to be able to point to true privacy protection in this area, you should apply the same procedure to all cookies*."

In 2009 **Yahoo!** has said that "*Last year, we committed to anonymizing the data we collect about your searches after 13 months. We are now reducing our retention time to 90 days with limited exceptions for fraud, security, and legal obligations*" and this means the deletion of the entire IP address. But the Working Party says that Yahoo! has not provided enough information on how it intends to handle cookies and other unique identifiers.

At this point, my considerations about this topic are the following ones: I see in the companies' replies data retention periods from 6 to 18 months…. These periods are considered still extremely long by the privacy autorities, but do you remember

---

[29] See note 2.
[30] *http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm.*

their data retention periods available to law enforcement authorities, that is from 30 to 60 days?

This difference is embarrassing!

But how can we contradict a business analysis? Retain data for the needs of the community is not a profitable deal!

7.2.2.2 Facebook's situation

With the coming of the social network, the issue of data retention has become more and more important.

On the other hand the new players seem to be aware of that. In fact this is Facebook's policy:

> **Special Provisions Applicable to Users Outside the United States**
>
> We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws[31].
>
> ***Responding to legal requests and preventing harm***
>
> *We may share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good-faith belief that the law requires us to do so.* ***This may include responding to legal requests from jurisdictions outside of the United States where we have a good-faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction and is consistent with internationally recognised standards****. We may also share information when we have a good-faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves and you from violations of our Statement of rights and responsibilities and to prevent death or imminent bodily harm[32].*

And yet, at the same way, these declarations remain statements of principle because the existing data are retained for much shorter periods (usually 90 days) than the UE Directive ones.

---

[31] *http://en-gb.facebook.com/legal/terms.*
[32] *http://en-gb.facebook.com/about/privacy/other.*

7.2.3 E-MAILS AND/OR DOCUMENTS ON SERVER ABROAD DATA CAPTURE

As already mentioned, even in such cases you can speak about a potential access without the co-operation of the ISP, where the Judicial Police have acquired in another way (e.g. phone tapping) the authenticating credentials to a certain repository (e.g. e-mail box, data storage service such as dropbox, etc…).

Here as well, first of all we must wonder if there are real problems of jurisdiction. In fact we suppose to be facing a postcard lying on the ground, with the printed side upwards, at 10 cm beyond the line of the Italian border: the Italian Police, without physically entering the foreign territory, may see it very well and therefore acquire the content.

This example makes us better understand the reason why, in the transborder access cases here reported, we are used to talk about a "magic window" that allows the Judicial Police to access with a simple click to a place different from the one they have jurisdiction (according to the traditional principles of the International Law), without trampling on the ground (because, through the usage of authenticating credentials, it's simply possible to copy the content leaving it – even on the computer- unchanged on that server).

So then the principle that sets off the power of disposal[33] as legal connecting factor, is actually able to return an acceptable legal parameter to the investigative action.

But also in the light of this principle **we will need to check, according to the mentioned principle of the violated or compressed freedom, which are however the guarantees to be recognized to the suspect, but according to the Law of the State where the suspect lives (usually the State conducting the investigation) and not the International Law.**

Thus, regarding the Italian experience, during the inspection of a place, the Criminal Procedural Code guarantees the right of defence in this way:

a. the notification of the order of inspection, if the suspect is present (art. 246 Criminal Procedural Code)
b. the notice to the suspect's lawyer, unless "*there is a justified reason to believe that the tracks or the other physical effects of the crime may be distorted*" (art. 364 Criminal Procedural Code)

[33] "*The formal power of disposal connects any data to the person or persons that obtain sole or collaborative access and that hold the right to alter, delete, suppress or to render unusable as well as the right to exclude others from access and any usage whatsoever*": see Discussion paper *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, p. 10 on *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/.*

c. the filing of the inspection report by the Prosecutor Office within 3 days, unless any delay (to be motivated with appropriate measures of the Public Prosecutor) for no longer than 30 days (art. 366 Criminal Procedural Code).

And then, for the hypothesis of the transborder access that we are discussing (also called online inspection), according to an investigative practice that is now developing in Italy and is in line with our Criminal Procedure Code, it will be possible to omit the guarantees sub a. (because by definition in the online inspection hypothesis the suspect it's not present) and sub b. (because usually there is a reasonable cause of the dispersion of evidence); while sub c. it will be necessary in any case to provide for the filing of the inspection report within 30 days, in order to allow the suspect to assert his right of defence.

[June, 2012]