Communication interception regarding Google, Microsoft & Yahoo! tools and electronic data retention on foreing servers: a legal prospective from the State which is conducting an investigation

Francesco CAJANI

Deputy Public Prosecutor
High Tech Crime Unit
Court of Law in Milan (IT)

Member of the technical and
scientific Committee of the
I.I.S.F.A. Italian Chapter

francesco.cajani@giustizia.it

www.iisfa.eu

1. "*A space with law but a cyberspace without law, just because it is cyber !*"

In the cyberspace the traditional country borders are cleared during the action made by the cyber criminal.

They come back only later, when the detectives try to trace that action searching digital evidence maybe left by the author and so useful for the investigations.

The main layout, even cultural – synthesized in the way of saying "*a space with law but a cyberspace without law, just because it is cyber !*" – is, as all the detectives know, in favour of the suspects.

Each time, we need to ask the involved States for a collaboration (through formal rogatory). But more important, the societies which provide electronic services and that have servers in those States, "in theory" would be inclined to a faster collaboration, but then they often attest that it wouldn't be possible according to "their" law.

That's what happens in general regarding many foreign societies but especially relating to the electronic services given by the three most important web societies in the world: Google, Microsoft and Yahoo!.

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

We more often find ourselves in front of opposite opinions.

On one side, I could talk about a "*no server no law*" opinion, that is the one that prefers the place where the web servers are based: and often, they are outside the European Community.

This first layout sustains that our respective laws (national or European) couldn't be enforced just because there aren't any web servers neither in Italy nor in Europe.

On the other side there is the opinion that I prefer and I hope I'll shortly have a support in the European Courts decisions: the "*no server but law"* opinion says that it's crucial the place where the web services are offered, no matter where the web servers are, even to the purpose of the law enforcement.

Besides, this second layout is in line not only with a correct application of any European laws but also with the internet jurisdiction analysis executed by the American Courts.

3. Two macro hypothesis

On the purpose of my topics, we need to verify if the concerned society has the availability of

a) communication channel
b) communication data

a) a society with communication channel availability

We can find here all the three already mentioned societies, because a flow of communications among people is produced through Google, Microsoft or Yahoo! e-mail systems.

Often, these people are both present in our State, but they use an e-mail system based abroad: in this way more often it happens what we mentioned before referring the "*no server no law*" opinion.

We all know that, referring national societies, enforcing the Judge's order it's possible to request that the e-mails sent to the intercepted account are redirected to the judicial police account: that allows not only a cost saving but even the change to start the inteceptions in reasonable short times.

Instead referring the e-mails *@.com*, this mechanism often becomes impossibile to execute.

Let me explain what I mean: my judicial police go to notify interception order to **Google Italia** or **Microsoft Italia** (both with registered office in Milan) and, as result, what do we have?

"*We are sorry but the servers are in Usa, so please ask for the interception with a rogatory!*"

So, it doesn't sound good if I'm investigating a murder or kidnapping.

Only **Yahoo! Italia** (which has the registered office in Milan, too) has a software - called *Yahoo! Account Management Tool* - that allows such e-mail interceptions, but with some limits. And with some problems, as it happens in one of our investigation which will be explained later.

b) a society with communication data availability

This hypothesis refers data regarding the Internet access, such as log files.

According to the Italian experience, **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 even to *hotmail.com* ones.

At first **Google Italia** talked about the need of a rogatory for any request in a way: then they have changed their policy providing all the requested data but only if there is an order from the Italian Public Prosecutor (and not only simply 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 server, at the moment this society doesn't feel to be allowed to communicate it to the Italian Judicial Autority.

Instead **Yahoo! Italia** asks for a rogatory only in some cases.

Anyway, for some of these three societies an important problem regarding this data retention must be taken into consideration.

4. Some preliminary enquiries

Referring the two profiles just clarified, each time we need to acquire some important information in order to face the problem better as investigators.

More precisely, we need to know

- where the society has his own web servers,
- where the society has the main legal registered office,
- if the society has an operating branch in the State where the investigation is conducted (and which law this branch is subjected to), as it happens with Google, Microsoft and Yahoo! (which have a lot of them in the European Communities),
- if there are some people, by these operating branches, who have the change of a concrete management.

5. "*Internet law and regulation*": the Internet jurisdiction analysis executed by the American Courts

But, even if we agreed with the "*no server no law*" opinion, what would happen in an American Court?

This is the meaning of my question: you are an American society also based in Europe, you tell me that your web servers are in one of US states (for example: California) and therefore you are not subjected to the European laws.

Well, could you say the same thing to a Judge summoning you in a Court of a different US state (for example: Arizona)? Or, arguing on the other side, could an Italian society say the same thing to a Federal American Court (that is: "*sorry, our servers are in Italy?*"). I don't think so…

Let's make a note about the Internet jurisdiction analysis executed by the American Courts. As you know[1],

> << U.S. courts have developed two general lines of analysis in determinig 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 *[Zippo Manufacturing. Co. v. Zippo Dot Com. Inc., 952 F Supp 1199 (WD Pa 1997)].*
>
> The second analysis (called "**effects test**") seeks to determine to what extent a defendant's intentional conduct outside the forum state *[Calder vs Jones, 465 U.S. 783 (1984)]* >>.

So, for a lot of years the U.S. state courts have been processing a very undisputed analysis stating the US jurisdiction even if the web site is based on a server in another country!

> << The cases discussed above demonstrate 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 the defendant conducts over the Internet and place it on a continuum ranging from "passive", where no business is conducted, to "clearly conducting business". **The**

[1] G.J.H. Smith, *"Internet law and regulation",* Sweet and Maxwell, 2002 (3rd edition), pp. 347-349.

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 defendant's intentional conduct was calculated to cause harm to plaintiff within the forum state. **Where a defendant "purposefully directs" his activities at the jurisdiction, he may be liable to suit for any injury relating to or arising from those activities >>**

7. Which obligations and national laws can we expect observance of?

At this point, regarding the topics I'm dealing with, the important question is: "*which obligations and national laws can we expect observance of?*"

I quote two real important ones in the Italian experience, according to our laws.

1. First of all, the **electronic communication rules** (Legislative Decree of 1st August 2003 n. 259) with EC origin in the four Directives underneath indicated:

   - **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)
   - **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)
   - **DIRECTIVE 2002/21/EC** OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)
   - **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)

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 by competent national authorities, as it is also said in the Article 6 of the EC Directive 2002/20/EC.

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.

ANNEX

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

According to these American societies, there are some US laws that will prevent themselves from imparting anyone data regarding communications of their users.

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, 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?

2. Secondly, we could expect the observance of the **data retention rules** (Legislative Decree of 30th May 2008 n. 109) with EC origin in the 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).

> ***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**
>
> 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 (6th 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.

However, it clearly comes out even in the following important opinion that any EC rules can be applied to the ones who turn their services to European citizens living in any EC States:

> "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 center"[2].

And therefore, on the purpose of my topics, it would mean that the obligations of data retention would be also applied to Google, Microsoft and Yahoo!.

8. Yahoo! Italia vs. **Public Prosecutor's Office in Milan**

As we have already mentioned, this was the situation referring Yahoo! Italia.

His base principle is called "Net Citinzenship", that can be better explained in the following way: when the Italian user registers an account from the webpage *yahoo.it*, he can choose which legislation to subject his e-mail box.

There is a software (called ***Yahoo! Account Management Tool*** and used by all the Yahoo! branches) which gives back the data of e-mail boxes (@*yahoo.it* and/or @*yahoo.com*) but only from users who chose the Italian law.

As I explained before, we can intercept these emails even without rogatory.

At the end, they had a 30/45 days of data retention (against a period of 12 months, which has already provided by the Italian Law since 2005 before the implementation of the Directive 2006/24/EC realized with the Legislative Decree of 30th May 2008 n. 109).

As a result we have a huge damage of the inquiries.

This happened till the *casus belli* took place in 2007.

The Officers of the Milan Financial Police called "Gruppo Pronto Impiego" had a Yahoo! mailbox under interception without any results. That means: no e-mails received at all, as we could see as investigators.

We arrested the suspect, a romanian phisher, who provided us the access credentials to mailbox which had been intercepted. We discovered that instead there were a lot of still lying messages, received in the period when the mailbox had been subjected to interception.

We ensured that a lot of people could enter the *Yahoo! Account Management Tool* from the several European branches of Yahoo!

This fact could damage the users' privacy and not only the police investigation…

We transferred the indictment to the Italian Privacy Authority, who confirmed our technical investigation and the juridicial layout.

Meanwhile Yahoo! Italia attorneys have communicated that the society will spontaneuosly conform to the above mentioned Legislative Decree of 30th May 2008 n. 109 so that it will retain log files for 12 months. That will happen not only for the Italian Judicial Authority requests but also for the ones of the other EC states (starting from 21st November 2007).

In my opinion, it couldn't be different: we are in presence of societies which must be included in the Article 3 of the 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).

---

[2] Peter Schaar, President Article 29 Data Protection Working Party, 16 May 2007.

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.

For such reasons and indipendently from the allocation of the servers, they are receivers of the preceptive obligations of the Italian and EC data retention rules …. pace the American law!

9. The present situation regarding Microsoft data retention periods

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.

The present situation, regarding the Italian experience, consists in Microsoft data retention periods not in line with the EC Directive, because it gives back informations about its e-mail boxes only about the last 60 days.

Anyone has a basic experience in cybercrime investigations can understand how short this period is!

The solution is not surely the one to make the investigative contacts faster, just because we can need to request data from this American society after having received information from other national Internet Service Provider: infact the results of these latest information, arrived at us after a period of time that is very often over 60 days, can refer to Microsoft users.

So, this dynamics effectively creates enormous damages to the investigations in progress in the EC States.

10. Conclusions

Data retention and a faster way to enable the wiretap of e-mails *@.com* need to support costs, but can we affirm that economical reasons can prevail over the defence of the people's rights which were damaged by (cyber)crimes?

Reasoning in terms of balance sheet, the business costs not supported by these societies are changing into higher social costs. And where are the profits? In the criminal association's pockets!

Nowadays we often talk about the Internet as a space of freedom… we have a lot of EC laws, yet there are many people who pretend not to see them, hiding behind a "cyberspace virtuality" which is only outward and that feeds not only profits but even crime.

As a Public Prosecutor, who is keen on information technologies, my wish and my hope is that everybody can rediscover the classical meaning of Freedom, which for the ancient Greeks "*was meant as the obedience to Law*"[3].

Nevertheless, despite all that and regarding the situation of any web society with server in the USA, we need to recall that USA ratified (and in this way they set a limit to their sovereignty) the 2001 Council of Europe Convention on Cybercrime, which provides for two precise obligations of cooperation (artt. 33 and 34).

[3] De Romilly, *La loi dans le pensèe grecque*, p. 23: this Author remarks the way used by the historian Herodotos (*The Histories*, VII, 104) to describe the Greek citizens ("*if it's true that they are free, they are not free for everything: a master dominates them, the Law, for which they have a fearful respect").*

Article 33

Mutual assistance in the real-time collection of traffic data

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.

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.

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 – as Italy has recently done (Law of 18th March 2008 n. 40) – ratified this Convention, specific duties rose. As the ancient Romans said and as the rules of the International Law remind us: *pacta sunt servanda*.

In particular, whereas US societies continue to consider themselves not applied by the European laws, the national Judicial Autorithies will act within the law in a reasonable and proper way[4] and will insist for an action[5] not only of the European administrative Authorities but even of the American ones, even in order to obtain a correct enforcement of the 2001 Council of Europe Convention on Cybercrime.

[6th March 2009]

[4] The latest episode (2nd March 2009) is the following: < A court in Dendermonde, Belgium, today found Internet company Yahoo guilty of withholding personal account information linked to Yahoo e-mail addresses. The court told the company to cough up a €55,000 fine right away and an additional €10,000 for each day it keeps refusing to hand over the user data (or $69,197 and $12,590, respectively). Yahoo got fined for its unwillingness to cooperate in a cyber-criminal investigation which prompted Belgian authorities to subpoena detailed account data for a number of e-mail addresses used by a gang of alleged internet cons. Yahoo's defense was that it would only respond to requests from American authorities, while the Belgian investigators claim it should turn over the data at their request too because the company operates its services in Belgium. Also worth noting is that the judge is being quoted as saying that this procedure for requesting data "*poses absolutely no problem with Google and Microsoft*". The court ruled in favour of the investigators: Yahoo got the maximum penalty > (*http://www.techcrunch.com/2009/03/02/yahoo-fined-by-belgian-court-for-refusing-to-give-up-e-mail-account-info/).*

[5] According to Article 10 of the Directive 2002/58/EC, "*Member States shall ensure that the Commission is provided on a yearly basis with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network. Such statistics shall include … the cases where requests for data could not be met".* Besides the Italian Legislative Decree of 30th May 2008 n. 109 provides fees from 50.000,00 to 150.000,00 Euros in case of not retention of data for 12 months.