ARTICLE:

INTERCEPTION OF COMMUNICATIONS: SKYPE, GOOGLE, YAHOO! AND MICROSOFT TOOLS AND ELECTRONIC DATA RETENTION ON FOREIGN SERVERS: A LEGAL PERSPECTIVE FROM A PROSECUTOR CONDUCTING AN INVESTIGATION[1]

By **Francesco Cajani**

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.[2]

'No server no law' v 'no server but law'

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, 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.*

[1] *This article is adapted from the speech of the author at the First Strategic Meeting on Cybercrime organised by Eurojust in Athens, 23-24 October 2008 (many thanks to Luisa and Valeria Viganò for the review). For the press release, see http://www.eurojust.europa.eu/press_releases/2008/30-10-2008.htm.*

[2] *Declan McCullagh, 'Skype: We can't comply with police wiretap requests', cnet news, 9 June 2008, available at http://news.cnet.com/8301-13578_3-9963028-38.html.*

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.

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.

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 was not possible in this case to enforce an order issued by the judge. The order that could not be enforced, requested that the e-mail accounts be intercepted by having the e-mail traffic redirected to the judicial police account. This method reduces costs, and permits the interception to begin quickly. This method is used when making similar requests to the national ISPs with servers in Italy. The alternative mechanism is for the judicial police to notify Google Italia or Microsoft Italia (both with registered offices in Milan) of the interception order. 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.

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 requested, providing the request is accompanied 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 server, Google does not consider it is permitted to communicate it to the Italian Judicial Authority. In comparison, Yahoo! Italia request a rogatory, but only in some cases.

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.

Jurisdiction analysis as applied in the United States of America

If the 'no server no law' opinion is accepted, it will be interesting to know what view an American judge would take. The scenario is as follows: 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

The closer the internet activities are to 'clearly conducting business', the more likely that a US court will exercise personal jurisdiction.

subject to the laws of the Member State in which they have an office. 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 US Court (for example: Arizona). It is debatable whether a US judge will accept such an argument. Consider how the judges in the US analyse internet jurisdiction.[3] Judges in the US have 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.[4] The second analysis, called the 'effects test', seeks to determine to what extent a defendant's intentional conduct takes place outside the forum State.[5] So, for a number of years, the US state courts have been using an undisputed analysis, providing for US 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 US forum state sufficient to subject him or her to general jurisdiction, may nonetheless be subject to personal jurisdiction in the US based on two broad theories of 'specific' personal jurisdiction. Under the *Zippo* 'sliding scale' analysis, a US 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 US 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.

Obligations and national laws to observe

At this point, the important question is to identify the obligations and national laws that we can be expected to observe. In Italy, the provisions of Decreto legislativo 1° agosto 2003, n. 259, Codice delle comunicazioni elettroniche[6] (Legislative Decree of 1st August 2003, n. 259 electronic communication rules) are fundamental. These rules have their origin in four EC Directives.[7] An important step has been taken by the Italian Ministero dello Sviluppo Economico (Ministry of Economic Development and Telecommunication), in that it has recently provided a written opinion (note of 12 September 2008, following a specific request of the Direzione Nazionale Antimafia) 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:

[3] *G. J. H. Smith, Internet law and regulation, (Sweet and Maxwell, 3rd edition, 2002), 347-349.*
[4] *Zippo Manufacturing Co. v Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa.1997).*
[5] *Calder v Jones, 465 U.S. 783 (1984).*
[6] *Pubblicato sulla Gazzetta Ufficiale n.214 del 15 settembre 2003.*
[7] *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 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.*

> 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:

> 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.

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).[8] 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 elephony 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.

It is clearly the opinion of Peter Schaar, President of the Article 29 Data Protection Working Party, that any EC 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'[9]

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

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

[8] *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.*

[9] *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.*

2006, which provides for two precise obligations of 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.
>
> 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,[10] specific duties arise. As the ancient Romans said, and as the rules of international law remind us: agreements must be kept (pacta sunt servanda).

In particular, whereas US ISPs continue to consider that EU laws do not apply to them, the national judicial authorities will continue to act within the law in a reasonable and proper way[11] and will insist for an action[12] not only of the European administrative authorities, of the US authorities, even if it is necessary to enforce the 2001 Council of Europe Convention on Cybercrime.

Yahoo! Italia and the Public Prosecutor's Office in Milan

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. The investigation authorities can intercept these e-mails, even without a rogatory. However, these e-mails only have a retention period of between 30 and 45 days, against a period of twelve months.[13] As a result, some investigations suffer. One occasion, a Yahoo! mail box was the subject of interception without any results. This meant that no e-mails were received at all. The investigators could see that no e-mails were received. The suspect, a Romanian phisher, was arrested. He provided the access credentials to the mail box that had been intercepted. It was discovered that there were a number of messages that had been received in the period when the mail box had been subjected to interception. During the period the mail box was the subject of interception, a great number of Yahoo! employees were free to enter the Yahoo! Account Management Tool from several of the European branches of Yahoo! This fact could damage the users' privacy, and not only the police investigation. The indictment was transferred to the Garante per la protezione dei dati personali (Italian Privacy Authority), who confirmed the technical investigation and that the

[10] *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).*

[11] *On 2 March 2009, a court in Dendermonde, Belgium, found Yahoo guilty of withholding personal account information linked to Yahoo e-mail addresses. This decision is in the process of being appealed. Note from the editor: it is antipicated that a full report on this case will be included in the 2010 issue of the journal.*

[12] *According to Article 10 of 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 OJl L 105, 13/04/2006 P. 0054 - 0063, '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'. See also Decreto legislativo 30 maggio 2008, n. 109, which provides fees from 50,000.00 to 150,000.00 euros for failing to retain data for 12 months.*

[13] *In accordance with 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; implemented by Decreto legislativo 30 maggio 2008, n. 109.*

legal approach taken by us was correct. Meanwhile, the attorneys for Yahoo! Italia indicated to the Public Prosecutor's Office in Milan that the company would spontaneously conform to Decreto legislativo 30 maggio 2008, n. 109, by storing log files for twelve months in future.[14] Apparently this will be enforced across all EC states, and started from 21 November 2007. In my opinion, it could not be different: we are in presence of societies which must be included in the provisions of article 3 of Directive 2002/58/EC:[15]

> 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 EC data retention rules.

Concluding comments

In conclusion, let me take a strictly personal view: each time I manage to come to Athens, I like to have a walk through the Agorà and go as far as the Monument of the Eponymous Heroes: this is the place where the legislation, decrees and announcements were shown, so that the Athenian citizens could see and know them. Well, today we have a lot of 'shown' laws, yet there are many people who pretend not to see them, hiding behind a 'cyberspace virtuality'. But this very cyberspace not only feeds such companies with their profits, but facilitates crime. There is a need to balance the rights of people that are the victims of a crime, against the econimics of the ISPs. The words by which the historian Herodotus of Halicarnassus described what Demaratos said of the Lacedemonians are relevant:[16]

> 'So also the Lacedemonians are not inferior to any men when fighting one by one, and they are the best of all men when fighting in a body: for though free, yet they are not free in all things, for over them is set Law as a master, whom they fear much more even than thy people fear thee. It is certain at least that they do whatsoever that master commands; and he commands ever the same thing, that is to say, he bids them not flee out of battle from any multitude of men, but stay in their post and win the victory or lose their life.'

Many commentators have seen in this affirmation the first statement of that 'Government of the Law', according to which the existence of a law distinguished the Greeks from the non-Greeks, and for this reason defined 'barbarians': therefore, in those times, for the Greeks:[17]

> Du Démarate d'Hérodote au Platon de la lettre VII, en passant par le Thésée d'Euripide, la tradition est bien la même. Elle implique un sens aigu de cette loi comune que les citoyens avaient su se donner et dont ils attendaient à la fois le bon ordre et la liberté. Pour eux, déja, la liberté se définissait comme l'obéissance aux lois.
>
> Of Démarate from Herodotus to Plato of letter VII, while passing by Theseus of Euripides, the tradition is the same. It implies an acute sense of this common law that the citizens had known to be given and from which they expected to both order and freedom. For them, freedom is already defined as obedience to the laws.

Today, we often talk about the internet as a space of freedom. As a Public Prosecutor, who is fond of information technologies, my wish and my hope is that this 'freedom' can really come true. The danger of a different concept of freedom, meant as the absence of laws, is a barbarity to be opposed.

Francesco Cajani is a Deputy Public Prosecutor in the High Tech Crime Unit at the Court of Law in Milan. He is also member of the Technical and Scientific Committee of IISFA (International Information Systems Forensics Association) – Italy Chapter (http://www.iisfa.eu).

francesco.cajani@giustizia.it

[14] *The Request for Archiving (not to prosecute and to close the case) was submitted to the court on 16 October 2008, and agreed by the judge, Dr Gaetano Brusa, on 25 March 2009. The Request is published at the end of this article.*

[15] *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.*

[16] *The Histories, VII, 104. (Translation of G. C. Macaulay, available at http://www.gutenberg.org/files/2456/2456-h/book7.htm).*

[17] *Jacqueline de Romilly, La loi dans le pensèe grecque, (1971, Belles letters, Paris), 23.*

N. 43083/07 R.G.N.R. mod. 21

Procura della Repubblica

presso il Tribunale di Milano

RICHIESTA DI ARCHIVIAZIONE

~ artt. 408/411 c.p.p., 125 e 126 D.Lv. 271/89 ~

Al Giudice per le indagini preliminari

presso il Tribunale di Milano

Il Pubblico Ministero

visti gli atti del procedimento penale indicato in epigrafe, iscritto nel registro di cui all'art. 335 c.p.p. in data il 23 ott 2007 nei confronti di:

M.M.

Difeso di fiducia […]

per l'ipotesi di reato:

- artt. 169 D.lgs. 196/2003, 81 cpv. c.p. accertato in MILANO in data 2 ottobre 2006 e permanente fino al luglio 2008 (data di adempimento delle prescrizioni impartite dall'Autorità Garante per la protezione dei dati personali).

PREMESSO CHE

1. Le indagini condotte dalla Procura della Repubblica di Milano (nascenti dall'impossibilità di fatto di concludere gli accertamenti di polizia giudiziaria alla luce di quanto denunciato dalla persona offesa in data 12.9.2005[1]) hanno accertato, relativamente alla condotta dell'indagato - nella

[1] Trattasi di invio di immagini pornografiche alla ragazza del denunciante, tramite utilizzo abusivo – ad opera di soggetti terzi non identificati (attesa la risposta negativa di Yahoo! Italia s.r.l. ai CC – Stazione di Bresso, datata 10 febbraio 2006, considerato il periodo di conservazione dei *files* di *log*

sua qualità di **amministratore delegato della società Yahoo! Italia s.r.l. (titolare del trattamento dei dati**, come risulta dal prescritto Documento Programmatico della sicurezza, p. 27) - la **mancata adozione delle misure minime di sicurezza** (previste dall'art. 33 del D. Lgs. 196/2003 – Codice privacy) **a protezione di dati personali riconducibili agli utenti dei servizi di comunicazione elettronica offerti dalla società Yahoo! Italia s.r.l.** (avente sede legale in Milano).

Più precisamente, nonostante la predisposizione del richiamato D.P.S. (peraltro redatto solo in data 2 ottobre 2006), veniva accertata – anche a seguito di una apposita ispezione dei sistemi informatici in uso alla società delegata al Gruppo Pronto Impiego della Guardia di Finanza di Milano - una **inidonea regolamentazione degli accessi all'applicativo denominato *Yahoo! Account***

---

riguardante "*solamente gli ultimi 30 giorni dalla data dell'accertamento*") della casella di posta elettronica *@yahoo.it* in uso alla persona offesa. Fatti di cui al p.p. 78193/05 mod. 44 in atti, in relazione al quale – anche a fronte di un provvedimento di diniego del GIP di acquisizione di ulteriori e diversi *files* di *log* (essendo decorsi i termini di 12 mesi così come previsti dal previgente combinato disposto degli artt. 132 commi 1 e 4 D.Lgs. 196/2003) - è stata richiesta l'archiviazione.

Più in particolare, l'impostazione dogmatica sostenuta da questa Procura – sotto la previgente normativa ex art. 132 Codice *privacy* - faceva leva sul dato sistematico al fine di ritenere comunque consentita una richiesta al GIP anche decorso il termine di 12 mesi (dal momento che: il combinato disposto degli artt. 132 commi 1 e 4 D.Lgs. 196/2003 - come modificato dalla l. 155/2005 - non poneva un limite massimo per la richiesta al GIP dei dati relativi al traffico telematico, prevedendo solo che "dopo la scadenza" dei 6 mesi il PM non potesse più autonomamente provvedere all'acquisizione; l'obbligo di conservazione dei richiedendi dati era pari ad "mesi dodici" ma ciò non escludeva che essi fossero conservati dai gestori telefonici per un periodo più lungo", come del resto ipotizzabile alla luce della "moratoria" fino al dicembre 2007, successivamente prorogata), salvo poi essere legittimamente disattesa dal gestore. Tale impostazione tuttavia trovava ostacolo nella seguente motivazione del GIP: "*seppure la norma non contiene un esplicito divieto all'acquisizione dei dati anche oltre il termine di conservazione previsto (supponendo che essi siano stati effettivamente conservati), trattandosi di disposizioni eccezionali perché limitative del diritto alla privacy – alla cui tutela esse sono improntate non è ammissibile una interpretazione estensiva, oltre i casi espressamente previsti, determinandosi altrimenti una'indebita compressione del diritto sopra menzionato* ." Il provvedimento di rigetto è stato confermato dalla Suprema Corte di Cassazione con declaratoria di inammissibilità dell'impugnazione proposta dalla Procura: nel parere del Procuratore Generale, sul punto si legge: "*la pur plausibile interpretazione del ricorrente, tuttavia, non è così cogente da negare altrettanta plausibilità all'interpretazione fatta propria dal decidente e posta a base del provvedimento impugnato [..]. Ciò, allora, già basta per negare fondamento alla sollevata deduzione di abnormità. Invero una pronuncia giudiziale può considerarsi abnorme quando sia del tutto anomale, sostanziandosi in una decisione che per la singolarità e stranezza del suo contenuto sia al di fuori dei poteri degli organi decidenti e non essendo previsto contro di essa un apposito rimedio, il ricorso alla Corte Suprema ha lo scopo di accertare e dichiarare l'abnormità del provvedimento e la rimozione in tal modo di una situazione altrimenti insanabile (Cass. Sez. V^ 19.6.91, SERAFINI e riff. Ivi contenuti) [..] Nella specie, per contro, la possibilità di decidere sull'autorizzazione senza necessariamente accedere alla richiesta del PM (già essendo errata – secondo la stessa sentenza n. 19278/05 invocata dal ricorrente – l'idea che il giudice debba atteggiarsi ad organo di mera ratifica dell'attività della parte pubblica), non è contestata neppure dal ricorrente (stante il potere che al giudice discende dall'art. 132 del D.L.vo 196/03)".*

Management Tool (cd. *Legal Tool*, che di fatto consente a Yahoo! Italia s.r.l. l'interrogazione dei dati relativi alla fornitura di servizi di comunicazione elettronica ai propri utenti, al fine di soddisfare le richieste della Autorità Giudiziaria) dal momento che

- di fatto, **persone non rientranti nel richiamato D.P.S.** (come incaricati del trattamento) quali F.M.[2] **nonché persone presso gli uffici del *Customer Care*** (peraltro allocati in uno Stato diverso, anche se comunque ugualmente soggetto alla normativa comunitaria)[3] **potevano avere liberamente accesso al richiamato applicativo**;

- il concreto funzionamento di tale programma (che consente direttamente, da parte di Yahoo! Italia s.r.l., un trattamento dei dati personali degli utenti) non poteva essere verificato,[4] e la richiamata società non era conseguentemente in grado di produrre una

---

[2] "*D.: Vuole specificare chi siano i soggetti abilitati ad utilizzare il "Legal Tool" o altrimenti detto "Yahoo! Account Management Tool"?*

R.: All'accesso all'utilizzo del Legal Tool è abilitato, oltre a me, anche il dott. F.M., in qualità di Legal Secondee, preciso che il dott. F. non è un dipendente della Yahoo! Italia, ma un collaboratore esterno. Ciascuno di noi due accede al sistema mediante l'inserimento di una personale "Yahoo! ID" che contraddistingue in maniera univoca chi accede al servizio. Pertanto il sistema è in grado di determinare in maniera precisa chi fruisca del servizio. Nessun altro è abilitato in tal senso" (s.i.t. C. del 12.2.2007 - dichiarazioni rese al PM).

[3] *"D.: Ha conosciuto la signora S.F.?*

R.: Si la conosco, in quanto quando ho iniziato a collaborare per Yahoo! la signora F. era l'assistente dell'allora General Counsel P. ed era la persona addetta all'utilizzo del Legal Tools per il riscontro delle richieste pervenute dalle Autorità Giudiziaria. All'epoca del mio arrivo in Yahoo! autorizzati all'utilizzazione dei Legal Tools in Italia erano l'avvocato P. e la signora F.. Non ricordo a quando risale la mia abilitazione ad interrogare i Legal Tools, in ogni caso quando anche P. si è allontanato da Yahoo! sono rimasto l'unico abilitato. Faccio presente tuttavia che la signora F. è stata trasferita all'ufficio "Customer care" di Dublino, e per tale sua funzione ancora oggi gode della possibilità di accedere al Legal Tools anche sui dati italiani, questo per motivi di assistenza clienti, quali il recupero delle password, preciso altresì che l'ufficio legale italiano ha il precipuo compito di rispondere alle richieste delle Autorità italiane e essenzialmente per questa finalità è nato il Legal Tool. Preciso altresì che tale applicativo nasce nel 2001 e viene da me utilizzato solamente per tale finalità. Prendo atto che P. ha indicato il 2003/2004 come data di installazione del Legal Tool ma sul punto potrei sbagliarmi io.

D.: Attualmente quali sono le altre persone abilitate ad accedere al Legal Tool?

R.: Che io sappia attualmente, oltre a me e la signora F. è abilitata la dottoressa C.F., che arriva in Yahoo! il mese di marzo 2006. Non ricordo di preciso quando P. lasciò Yahoo! prendo atto che ha dichiarato nell'ottobre 2005. In ogni caso da quando P. lasciò Yahoo! fino all'arrivo della C. sono stato l'unico ad essere abilitato all'accesso al Legal Tool, con la precisazione che ho già fatto con la possibilità della F.." (s.i.t. F. del 27.6.2007 – dichiarazioni rese al PM).

[4] *"D.: Il sistema di Yahoo! Inc. riconosce l'indirizzo IP da cui viene effettuata la registrazione indipendentemente dalla lingua prescelta?*

adeguata certificazione (con relativa assunzione di responsabilità circa la corrispondenza tra il dato trattato e il dato fornito all'esito della interrogazione) laddove chiamata a comunicare alla Autorità Giudiziaria le informazioni richieste;

- peraltro lo stesso applicativo, per una discutibile *policy* aziendale,[5] era programmato per non fornire il dato richiesto dalla Autorità Giudiziaria laddove l'utente, pur avendo stipulato il relativo contratto di servizi di comunicazione elettronica in Italia, abbia scelto che lo stesso sia regolamentato da una normativa nazionale diversa da quella italiana;[6]

- **non era possibile, per la società Yahoo! Italia s.r.l. (sebbene titolare del trattamento), avere accesso ai *log* delle operazioni di consultazione** (che dunque potrebbero essere liberamente poste in essere, senza alcun timore di venire successivamente identificati, da soggetti comunque non autorizzati dalla società italiana sulla base delle relative nomine rilevanti ai sensi del D.lgs. 196/2003) dal momento che trattasi di programma volto ad interrogare dati di fatto presenti su *server* esteri;[7]

Tale programma, di fatto "incontrollabile" da Yahoo! Italia s.r.l. (sotto il duplice profilo degli verifica degli accessi e dei risultati da esso generati), aveva comportato – in almeno un caso accertato – la **mancata comunicazione, alla Autorità Giudiziaria richiedente, del flusso delle comunicazioni relative al traffico telematico (scambio di comunicazioni *e-mail*, comunque ritrovate dalla polizia giudiziaria delegata in quanto ancora giacenti nella casella di posta elettronica *@yahoo.it* dell'indagato anche se non comunicate da Yahoo! Italia s.r.l. nei 15 giorni delle operazioni di intercettazioni)**[8], con notevole pregiudizio alle indagini in corso.

R.: Al momento non sono in grado di rispondere, anche perché i criteri in base ai quali questo Tool restituisce il dato sono a me noti solo in quanto mi sono stati riferiti dalla casa madre. Come già detto non c'è un vero e proprio manuale tecnico-operativo nel quali vengono attestati da Yahoo! Inc. i criteri di ricerca di tale tool sul database di Yahoo!" (s.i.t. C. del 12.2.2007 - dichiarazioni rese al PM).

[5] Cfr. p. 19 D.P.S.

[6] Cfr. comunicazione del Sostituto Procuratore Gianluca Braghò del 25.6.2007 per fatti relativi ad un procedimento penale in carico al Suo Ufficio.

[7] *"D.: sussiste un'attività relativa agli accessi a caselle di posta elettronica @yahoo.it che possa essere documentata, con creazione dei relativi files di log, ad opera di server di proprietà di Yahoo! Italia s.r.l. o comunque di server di proprietà del gruppo Yahoo?*

R.: In Italia non esiste alcun server per erogare i servizi di Yahoo agli utenti italiani nel senso che la rete dei server è centralizzata all'estero ovvero esistono diverso "server farm" sia in Paesi europei (ad esempio a Londra e in Irlanda) che in America." (s.i.t. M.M. del 12.2.2007 – dichiarazioni rese al PM).

[8] Cfr. verbale di operazioni compiute dal PM in data 30 agosto 2007 e successiva annotazione di PG del 4 ottobre 2007 (trattasi di indagini relative ad organizzazioni criminali transnazionali dedite all'attività di phishing).

Secondo l'impostazione di questa Procura, anche da tale "incontrollabilità" dell'applicativo denominato *Yahoo! Account Management Tool* derivava, di contro, un indebito trattamento di dati personali, potendo essere erroneamente comunicati alla Autorità Giudiziaria informazioni diverse da quelle effettivamente presenti sui *server* esteri, con notevole pregiudizio per gli utenti interessati, anche considerata la diffusività dei servizi di comunicazione elettronica offerti da Yahoo! Italia s.r.l.

2. Ai sensi del combinato disposto di cui agli artt. 169 comma 2 D.lgs. 196/2003 e 22 comma 1 D.lgs. 758/1994**,** in data 23 ottobre 2007 si trasmettevano di conseguenza all'Autorità Garante per la protezione dei dati personali gli atti relativi al procedimento penale in oggetto, utili per le opportune valutazioni sulla necessità di impartire – con specifico provvedimento - le prescrizioni necessarie ad eliminare quanto accertato.

L'Ufficio del Garante per la protezione dei dati personali veniva, nell'occasione, altresì sollecitato a prendere in considerazione quanto accertato da questa Autorità Giudiziaria ai fini delle proprie determinazioni all'esito della consultazione pubblica di cui alla delibera del 19 settembre 2007 relativa alle "*misure e accorgimenti a garanzia degli interessati in tema di conservazione di dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati*", dal momento che Yahoo! Italia s.r.l. (nonostante quanto indicato nel richiamato D.P.S. alla pagina 5 e sostenuto dal Direttore dell'Ufficio Affari legali[9] oltre che dall'amministratore delegato[10]) è **società che tratta dati personali connessi alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione** (art. 3 Direttiva n. 2002/58/CE).

---

[9] "*D: Siete a conoscenza dei limiti temporali dettati dalla vigente normativa in materia di conservazione dei files di log come disposto dall'art. 132 del D.L.Vo 196/2003? […].*

R. Sì, ne siamo a conoscenza ed in alcune occasioni ci siamo fatti portavoce presso la casa madre, attraverso tutta la procedura burocratica interna, dell'esistenza del testo di legge di cui si tratta. Tra l'altro ribadisco che, secondo l'interpretazione che Yahoo!Italia da alla norma, non riteniamo di aver contravvenuto al dettato normativo, proprio in virtù del fatto che non forniamo, come prevede la norma, servizi di traffico telematico" (s.i.t. C. del 14.9.2006 – dichiarazioni rese alla PG delegata).

[10] *"vorrei far presente che, tecnicamente, Yahoo! Italia s.r.l. non fornisce servizi di traffico telematico strettamente inteso se per traffico telematico si intende accesso alla rete internet. Con riferimento ai servizi di posta elettronica e messaggistica istantanea, Yahoo! Italia s.r.l. è solo licenziataria di tali servizi che, materialmente vengono forniti da Yahoo! Inc. con sede in California (USA). Siamo consapevoli dei problemi relativi alla "giurisdizione" di internet, e quindi quando un utente decide di aprire una casella di posta elettronica @yahoo.it sottoscrive una dichiarazione in tal senso. Premetto che, per accedere alla molteplicità di servizi offerti dal nostro portale, in sede di prima registrazione viene assegnato un ID univoco a ciascun utente; quando all'utente, in fase di registrazione, viene chiesta l'indicazione della lingua che dovrà essere utilizzata, in quel momento si identifica quello che gli americani chiamano " Net Citizen Ship" ovvero una sorta di "cittadinanza" nella rete. Il senso è che non è la società a dichiarare quale sia la propria giurisdizione ma è il cittadino che la dichiara al momento della sottoscrizione per cui se un cittadino chiede l'assegnazione di una casella di posta elettronica @yahoo.it, ma indica come lingua una diversa dall'italiano, gli vengono proposti i termini e le condizioni in relazione alla legislazione vigente nel Paese della lingua scelta"* (s.i.t. M.M. del 12.2.2007 - dichiarazioni rese al PM).

3. Dopo un formale sollecito datato 4 febbraio 2008,[11] il 2 aprile 2008 l'Autorità Garante comunicava[12] di aver provveduto ad adottare un provvedimento di prescrizione ai sensi dell'art. 169 comma 2 Codice privacy, al fine di adottare le misure di sicurezza che, sulla base degli accertamenti svolti dalla Procura, sono risultate non adottate (cfr. provvedimento del 13 marzo 2008 e nota del Dipartimento Attività Ispettive e sanzioni).

Inoltre, nella richiamata nota, il Dirigente del dipartimento attività ispettive e sanzioni presso il Garante per la protezione dei dati personali così concludeva, all'esito della relativa istruttoria:

> "*L'indagine della Procura di Milano [..] fa emergere alcuni elementi sulla liceità dei trattamenti che, seppur non compiutamente definibili nell'ambito della procedura di cui all'art. 169, 2° comma, del Codice, appaiono, in ogni caso meritevoli di approfondimento da parte dell'Autorità. [...]* ***Nondimeno, un approfondimento appare opportuno al fine di chiarire anche l'eventuale ambito di applicazione di altre disposizioni del Codice (ad es. l'art. 132) alle quali fa riferimento l'indagine della Procura di Milano****, ancorchè non inerenti alla materia delle misure minime di sicurezza, alla luce del provvedimento sulla sicurezza dei dati di traffico telefonico e telematico adottato il 17 gennaio 2008".*

RILEVATO CHE

- in data 27 settembre 2008 l'Ufficio del Garante comunicava che l'indagato, a seguito del puntuale adempimento alle prescrizioni impartite,[13] aveva effettuato il pagamento della sanzione (euro 12.500,00) pari al quarto del massimo dell'ammenda stabilita dalla norma violata;

- la documentazione depositata dai difensori dell'indagato in data 10.9.2008 (ovvero copia degli atti trasmessi al Garante al fine di adempiere alle prescrizioni impartite) ha consentito anche a questo Pubblico Ministero di verificare tale puntuale adempimento;

- non risultano profili di rilevanza penale ulteriori rispetto a quelli già oggetto di prescrizioni;

---

[11] Essendo scaduto il termine di 60 gg ai sensi dell'art. 169 comma 2 D.lgs. 196/2003 e 22 comma 2 D.lgs. 758/1994.

[12] Cfr. l'annotazione di segreteria in atti.

[13] Ovvero:

1. designare ad incaricati ai sensi dell'art. 30 del Codice privacy di tutti gli operatori addetti alla consultazione dei dati personali degli utenti Yahoo! mediante il sistema *Account Management tool;*

2. attuare, per il trattamenti relativi a detti dati, delle misure previste dalle regole 1-10, 12-14 e 27 del disciplinare tecnico di cui all'allegato B del Codice;

3. adottare un aggiornato Documento programmatico sulla sicurezza nei termini e nelle forme previste dalla regola n. 19 del disciplinare tecnico di cui all'allegato B) del Codice.

- peraltro la stessa società, in data 9 settembre 2008 ha comunicato al Garante che, "***anche ai sensi del recente Decreto Legislativo n. 109 del 30/05/2008, si è adoperata per approntare le misure tecniche necessarie a garantire il tracciamento e la conservazione dei dati del traffico telematico*** *(cd. files di log, dati relativi agli accessi effettuati dagli utenti alle Proprietà Yahoo![14])* ***per un periodo pari a 12 mesi****; allo stato risultano già disponibili i file di log decorrenti dalla data del 21 novembre 2007"*, precisando ulteriormente – con comunicazione a questa Procura del 10.9.2008 – che "*le suddette misure tecniche sono state adottate anche per le altre società europee del Gruppo le quali, a seconda delle diverse discipline locali, ne hanno dato specifica attuazione*".

INTERVENUTA

quindi, con l'adempimento ed il pagamento, l'estinzione del reato, così come previsto dall'art. 169 comma 2 Codice privacy

visti gli artt. 411 c.p.p., 125 D.Lv. 271/89

CHIEDE

che il Giudice per le indagini preliminari in sede voglia disporre l'archiviazione del procedimento e ordinare la conseguente restituzione degli atti al proprio ufficio

Milano, 16 ottobre 2008

IL PROCURATORE DELLA REPUBBLICA

Francesco CAJANI - Sost.

[14] Intendendo con tale definizione "*i servizi web-based offerti da Yahoo! per il cui utilizzo sia necessaria la preventiva registrazione degli utenti al sito istituzionale ..* www.yahoo.it*, tramite apposito modulo di iscrizione, ovvero la successiva identificazione mediante inserimento di username e password".*

Criminal proceedings no. 43083/07 R.G.N.R. mod. 21

Office of the Prosecutor of the Republic at the Court of Milan

---

REQUEST FOR ARCHIVING*

~ *artt. 408/411* Code of Criminal proceedings,
125/126 Legislative Decree no. *271/89* ~

To the Judge for preliminary investigations

---

* This is an official act to determine not to prosecute the defendant (the Managing Director of Yahoo! Italy s.r.l.) and to close the criminal case, in accordance with the provisions of the Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (Pubblicato sulla GU n.174 del 29-7-2003 - Suppl. Ordinario n.123) (Personal Data Protection Code (Privacy Code - Legislative Decree no. 196 dated 30 June 2003)), Section 169: 'Security Measures. 1. Whoever fails to adopt the minimum measures referred to in Section 33 in breach of the relevant obligations shall be punished by detention for up to two years. 2. A time limit shall be set either upon detecting the abovementioned offence or, in complex cases, by way of a subsequent provision issued by the Garante (i.e. Privacy Authority), for the offender to comply with the requirements referred to above. Said time limit shall not exceed the time span that is technically required; however, it may be extended in especially complex cases or else because of objective difficulties in complying, but it shall not be longer than six months. Within sixty days of the expiry of the above deadline, the offender shall be permitted by the Garante to pay one-fourth of the highest fine that can be imposed in connection with the administrative violation, on condition that the relevant requirements have been complied with. Compliance and performance of the abovementioned payment shall extinguish the offence. The body setting the time limit and the Public Prosecutor shall abide by the provisions made in Sections 21, 22, 23 and 24 of Legislative Decree no. 758 of 19.12.1994, as subsequently amended, insofar as they are applicable'. For the text of Italian Privacy Code (English version) see http://www.garanteprivacy.it/garante/document?ID=1219452.

at the Court of Milan

The Public Prosecutor

having regard to acts of criminal proceedings in the above mentioned request, entered in the register of criminal proceedings to be processed under art. 335 Code of Criminal proceedings on 23 October 2007 against:

M.M.

Defended in confidence [...]**

in the case of crime:

Arts. 169 Legislative Decree no. 196/2003, 81 paragraph 2 Criminal Code ascertained in Milan on 2 October 2006 and continuing until July 2008 (date of fulfilment of the requirements issued by the Authority for personal data protection).

WHEREAS

1. Investigations conducted by the office of the Prosecutor of the Republic in Milan (arising from the de facto impossibility of being able to conclude the criminal police investigation in the light of the complaint reported by the complainant on 12 September 2005)[1] pointed out, in relation to the suspect's conduct – in his powers

** This is addressed to the lawyer who is appointed by the defendant.

1. The issue is the sending of pornographic pictures to the girl that complained of unauthorised use – at the hands of third parties not identified (given the negative response of Yahoo! Italia s.r.l. to the Carabinieri of Bresso, dated 10 February 2006, given the storage period for the log files "only for the last 30 days from the date of ascertaining the crime") of the mailbox @yahoo.it given for the use of the person that is offended. Deeds as of criminal proceedings no. 78193/05 mod. 44 of the official records, for which – also in view of a measure by the GIP (Giudice per le Indagini Preliminari, i.e. 'Judge for the Preliminary Investigations') of refusing to collect additional and different log files (the term of 12 months having expired as provided for by the combined provisions of article 132 paragraphs 1 and 4 of Legislative Decree no. 196/2003) – archival was required.

More specifically, the dogmatic approach supported by this Prosecutor – under the previous legislation in accordance with art. 132 of the Privacy Code – was attempting to obtain the systematic data in order to deem, however, also allowed an application for the GIP even beyond expiration of the terms of 12 months (since the combined provisions of arts. 132 paragraphs 1 and 4 Legislative Decree no. 196/2003 – as amended by Law no. 155/2005 – do not put a limit on the request to the GIP of telematic traffic data, providing only that "after the expiration" of 6 months the PM (Pubblico Ministero, i.e. 'Public Prosecutor') could not independently enforce this acquisition; the obligation requiring the retention of data was for "twelve months" but this did not exclude the possibility that they were held by telephone operators for a longer period, as is conceivable in light of the "moratorium" until December 2007, (later extended) except where the data is legitimately disregarded by the operator. This approach, however, was hampered by the GIP for the following reasons: "although the rule does not contain an explicit prohibition to retain data beyond the specified retention period (assuming that they were actually kept), these provisions being exceptional, because they are restrictive provisions of the right to privacy – the protection of which they are aiming to – an extensive interpretation is not admissible, beyond the expressly provided cases, otherwise an arbitrary limitation of the above mentioned right".

as Managing Director of Yahoo! Italy s.r.l. (owner of data processing, as it turns out from the required Security Programmatic Document (Documento Programmatico della Sicurezza- DPS, p. 27) – the failure to adopt the minimum security measures (provided by art. 33 of Legislative Decree no. 196/2003 - Privacy Code) to protect Personal data referable to users of the electronic communications services provided by Yahoo! Italy s.r.l. (having their head office in Milan).

More specifically, despite the establishment of the recalled DPS (which was only drafted on 2 October 2006), it was ascertained – also further to a special inspection on computer systems in use at the company delegated to the Gruppo Pronto Impiego of Guardia di Finanza in Milan – inappropriate rules to control access to the application "Yahoo! Account Management Tool" (called "Legal Tool", which in fact enables Yahoo! Italia s.r.l. to perform inquiries on data related to the provision of electronic communications services to its users in order to meet the Judicial Authority requests):

The measure of rejection was confirmed by the Supreme Court of Cassation with a declaration of ineligibility of the appeal proposed by the Prosecutor: the opinion of the Attorney General, on the point reads: "while the applicant interpretation is however plausible, is not as binding as to deny similar plausibility to the interpretation of the decision-maker (here the GIP is meant) set at the base of the measure challenged [..]. This, then, is already enough to deny the foundation raised on deduction abnormity. Indeed, a court ruling can be considered abnormal when it is totally unusual, substantiating in a decision that for singularity and unusualness of content is outside the powers of the decision-making body, and not being against it foreseen an appropriate remedy, the appeal to the Supreme Court has the purpose to ascertain and declare the measure as abnormal and thus removing a situation otherwise irremediable (Cass. Sez. V of 19.6.91, SERAFINI and therewith included references) [..] In the present case, conversely, the possibility to decide on the authorisation without having to accede to PM's request (already being wrong – in accordance with the very ruling no. 19278/05 invoked by the plaintiff – the idea that the GIP should act as the body to mere ratification of the Public Prosecutor) is not disputed even by the applicant (given the power that derives to the GIP from art. 132 of Legislative Decree no. 196/03).

- In fact, people not addressed by the DPS (as in charge of data managing) as F.M.[2] as well as people at the offices of Customer Care (also allocated in a different Country, although still subject to the same Community legislation)[3] could have free access to the application at issue;
- The practical operation of this program (which allows the direct processing of personal data of users by Yahoo! Inc.,) could not be verified,[4] and the company was therefore not able to produce a proper certification (with assumption of responsibility on the correspondence between the data processed and the data provided as the result of the question) when summoned to provide the judicial authorities the information requested;

2 "Q.: Do you want to specify who are the persons entitled to use the 'Legal Tools' or otherwise known as 'Yahoo! Account Management Tool'?
A.: To obtain access the Legal Tool is enabled, in addition to me, Dr. F.M., as Legal Secondee. I clarify that F. is not an employee of Yahoo! Italy, but an external consultant. Each of us has access to the system by inserting a personal "Yahoo! ID" which uniquely identifies whomever accesses the service. Therefore the system is able to determine with precision who benefits from the service. No one else is authorized to do so." (Statements from C. to Public Prosecutor on 12.2.2007).

3 "D.: Did you know Mrs S.F.?
A.: Yes, I know her, because when I started to work for Yahoo! Mrs. F. was the assistant to the then General Counsel P. and was the person responsible for the Legal Tools for the investigation requests received by the Judicial Authority. At the time of my arrival at Yahoo! the use of the Legal Tools in Italy was authorized by lawyer P. and Mrs. F.. I do not remember to when, back in time, my authorization to examine the Legal Tools was given, in any case when P. quit from Yahoo! I was the only person enabled. I would point out however that Mrs F. was transferred to the "customer care" service in Dublin, and that it still possible to her to obtain access to the Legal Tools, also on Italian data, and this depends on her customer service related tasks, such as the password recovery, I also clarify that the Italian legal office has the principal task of responding to the demands of the Italian authorities, and primarily for this purpose the Legal Tool was created. I also point out that this application was created in 2001 and is used by me only for that purpose. I note that P. indicated 2003/2004 as the date of installation of the Legal Tool, but I might be mistaken instead.
Q.: Currently, who are the other persons entitled to obtain access to the Legal Tool?
A.: As far as I know now, apart from me and Mrs. F., Dr. C.F. is enabled, who arrived in Yahoo! in the month of March 2006. I do not remember exactly when P. left Yahoo! I note that he said in October 2005. In any case, since P. left Yahoo! until the arrival of C., I was the only one that was enabled to use the Legal Tool, with the clarification that I did with the possibility of F.." (Statements from F. to public Prosecutor on 27.6.2007).

4 "Q.: The Yahoo! Inc. system recognizes the IP address from which the registration is done regardless of the chosen language?

- Moreover, the same application program, in respect of a questionable company policy,[5] was programmed not to provide the data required by the judicial authorities where the user, despite having signed the contract for electronic communications services in Italy,[6] has decided that it is regulated by national legislation other than the Italian law;
- It was not possible for the company Yahoo! Italy s.r.l. (although the owner of the service), to have access to the logs of the enquiry operations (which could therefore be put in place freely, without fear of being identified later, by persons in any case not authorized by the Italian company on the basis of their specific appointment relevant to the Legislative Decree no. 196/2003) since this is a program aimed at questioning the factual data on foreign servers.[7]

This program, in fact "uncontrollable" by Yahoo! Italy s.r.l. (in point of view both of access and verification of the results generated by it), entailed – in at least one

A.: As of now I can not answer, also because the criteria on which basis this tool returns the data are known to me only because I have been so reported by the parent Company. As I have already said, there is no real technical and operational manual in which the search criteria of this tool on the database of Yahoo! are attested by Yahoo! Inc." (Statements from C. to Public Prosecutor on 12.2.2007).

5 See p. 19 D.P.S.

6 See Notification of Deputy Prosecutor Gianluca Braghò on 25.6.2007 for the facts relating to a criminal proceeding in charge to his office.

7 "Q.: Is there any activity related to access mailboxes @yahoo.it that can be documented, with its creation of log files, by servers owned by Yahoo! Italy s.r.l. or by a server owned by Yahoo Group?

A.: In Italy there is no server to provide services to Italian Yahoo users, in that the servers network is centralized abroad or there are different "server farms" both in European countries (for example in London and Ireland) and in America." (Statements from M.M. to Public Prosecutor on 12.2.2007).

recorded case –the failure to communicate to the Judicial Authority that requested the flow of communications on the network traffic (an exchange of e-mail, however, found by the police as yet delegated stored in the suspect's e-mail box @yahoo.it even if it was not provided by Yahoo!, Inc. in the 15 days of operational interceptions),[8] which had a remarkable detriment to the ongoing investigations.

According to this Prosecutor Office, even from this "impossibility to have control on" the application called Yahoo! Account Management Tool stemmed, in contrast, an undue treatment of personal data, being possible that information other than those actually present on foreign servers could be erroneously reported to the judicial authorities, with considerable damage to interested users, even given the broad diffusion of electronic communications services offered by Yahoo! Italy s.r.l.

2. Under the combined provisions of Articles 169 paragraph 2 of Legislative Decree no. 196/2003 and 22 paragraph 1 of Legislative Decree no. 758/1994, on 23 October 2007 the documents relating to the criminal proceedings in question were consequently sent to the Privacy Authority, in order to properly evaluate the need to

8 See minutes of operations carried out by the PM on 30 August 2007 and subsequent remark of PG (Polizia Giudiziaria, i.e. "Investigative Police"), 4 October 2007 (i.e. the investigation on transnational criminal organizations engaged in phishing).

provide – with specific measures – what provisions were necessary to remove the incorrect behaviour at issue.

The Privacy Authority Office was also urged to consider the findings of this judicial authority (i.e. the Prosecutor) for its own assessment of the results to the public consultation, and referred to the deliberation of 19 September 2007 on "measures and arrangements to ensure those concerned with regard to the retention of traffic data and telephone line for the purposes of investigation and prosecution of crimes", as Yahoo! Italy s.r.l. (and notwithstanding what is stated at page 5 of the mentioned DPS and stated by the Director of Legal Affairs[9] as well as by the Managing Director[10]) is a company that deals with personal data related to the provision to the public of electronic communication services over public networks of communications (art. 3 Directive 2002/58/EC).

3. After a formal reminder dated 4 February 2008,[11] on 2 April 2008, the Privacy Authority informed[12] Yahoo! Italy s.r.l. that it had taken action to adopt a prescriptive measure under Article 169 paragraph 2of the Privacy Code in order to adopt those

9 "Q: Are you aware of any time limit dictated by the current legislation on the retention of log files as per art. 132 Legislative Decree no. 196/2003? [...].

R. Yes, we are aware and on some occasions we have acted as spoke persons (the witness means they were proactive in making their parent company aware of) towards our parent company, through the entire internal bureaucratic procedure, on the existence of the text of the law at issue. Among other things I repeat that according to the interpretation that Yahoo! has of the rule, we do not believe that we have contravened the legal requirements, by virtue of the fact that we do not provide, in the normal course of events, traffic telematic services." (Statements from C. made to the delegated PG on 14.9.2006).

10 "I would point out that, technically, Yahoo! Italy s.r.l. does not provide traffic telematic services if strictly intended for traffic telematic means access to the Internet. With regard to electronic mail services and instant messaging, Yahoo! Italy s.r.l. license is only for those services that are actually delivered by Yahoo! Inc. based in California (USA). We are aware of the problems related to "jurisdiction" of the Internet, and then when someone decides to open a mailbox @yahoo.it, they sign a declaration to that effect. I beforehand state that in order to obtain access to the multitude of services offered by our portal, during the first registration each user is assigned a unique ID; when the user, during the registration phase, is asked what language shall be used, in that very moment is identified what the Americans call "Net Citizen Ship" or a kind of "citizenship" in the network. The meaning of this is that it is not the company who declares what its own jurisdiction is, but it is the citizen who declares it at subscription time, and if a citizen asks for the assignment of a mailbox @yahoo.it, but indicates a language different from Italian, he is proposed the terms and conditions related to the legislation in force in the country of the chosen language." (Statements from M.M. to Public Prosecutor on 12.2.2007).

11 As the deadline of 60 days in accordance with articles 169 paragraph 2 Legislative Decree no. 196/2003 and 22 paragraph 2 Legislative Decree no. 758/1994.

12 See the remark in answering acts.

security measures that, on the basis of investigations conducted by the Prosecutor, had not been enforced (see decision of 13 March 2008 and note of the Department Inspections and Sanctions).

Moreover, in that note, the Director of the Department of Inspections and Sanctions at the Privacy Authority concluded the results of its investigation as follows:

> "The investigation by the Milan Prosecutor [..] reveals some elements on the lawfulness of the treatments which, although not fully defined under the procedure provided for in art. 169 paragraph 2 of the [Privacy] Code, are in any case worthy of study by the Authority. [...] Nevertheless, a close examination also seems appropriate to clarify the scope of the application of other provisions of the Code (e.g. art. 132) which are referred to by the Prosecutor of the Milan investigation, even if not related to the matter of minimum security measures in the light of the decision on the telephone and telematics traffic data security adopted on 17 January 2008."

HAVING NOTED THAT

- On 27 September 2008 the Office of the Privacy Authority stated that the suspect, following the exhaustive fulfilment of prescriptions issued,[13] paid the fine

13 That is:

1. appoint agents in accordance with art. 30 of the Privacy Code of all persons involved in the consultation of the personal data of users Yahoo! through the account management tool;

2. implemented, for treatments related to these data, the measures envisaged by rules 1-10, 12-14 and 27 of the technical specification set out in Annex B of the Code;

3. adopt an updated paper on security in terms and forms required by Rule No. 19 of the technical specification set out in Annex B) of the Code.

(12,500.00 euros) equal to one quarter of the maximum fine value established by the rule infringed;

- The documentation filed by the defender's lawyers on 10 September 2008 (or rather copies of documents submitted to the Authority in order to fulfil the requirements given) has enabled this Prosecutor to ascertain the exact fulfilment;
- no further aspects relevant to the criminal law emerge in addition to those already subject to requirements or provisions;
- However, the same company, on 9 September 2008 informed the Authority that "even under the recent Legislative Decree no. 109 of 30 May 2008, it has been working to prepare the technical measures necessary to ensure the tracking and storage of electronic data traffic (i.e. log files, data related to users' access to Yahoo Properties)[14] for a period of 12 months, log files from the date of 21 November 2007 are already available", further stating – with communication to this Prosecutor on 10 September 2008 – that "these measures have been taken for other European companies of the Group which, according to various local provisions, have implemented them."

14 This means "the web-based services offered by Yahoo! for the use of which the users prior registration to the official website ... www.yahoo.it is required through an appropriate application form, or rather the subsequent identification by entering a username and password".

HAVING OCCURRED

therefore, with the fulfilment and the payment, the extinction of the crime, in accordance with art. 169 paragraph 2 of the Privacy Code

Viewed Articles. 411 of the Code of Criminal proceedings, 125 of the Legislative Decree no. 271/89

CALLS

that the judge for preliminary investigations should file the proceedings and order the return of documents resulting to its office.

Milan, 16 October 2008

THE PROSECUTOR OF THE REPUBLIC
Francesco CAJANI - Deputy.

The editor thanks Francesco Cajani and Ing. Franco Ruggieri, FIR DIG Consultants di Ruggieri Franco & C s.a.s., for taking the trouble to check this unofficial translation for accuracy. All mistakes remain those of the editor.

Postscript

The Judge at the Court of Milan (decree no. 223087/08 R.G. GIP of 24.3.2009) accepted this request in accordance with the provisions of article 169 of the Decreto Legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali (pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123) (section 169 of the Personal Data Protection Code (Legislative Decree no. 196 dated 30 June 2003)) since "le considerazioni in fatto e in diritto svolte dal P.M. vanno integralmente condivise" "regarding the facts and the law, the arguments of the Public Prosecutor are fully shared". With this decision of the Judge, the case can now be considered public and it can be published.
During the investigation, it was discovered that Yahoo! Italia s.r.l. failed to adopt minimum security measures (because a great number of Yahoo! employees were free to enter the Yahoo! Account Management Tool from several of the European branches of Yahoo!). The indictment was transferred to the Garante per la protezione dei dati personali (Italian Privacy Authority), who confirmed the technical investigation and that the legal approach taken by the Prosecutor was correct. After this, Yahoo! Italia s.r.l. decided to adopt the measures set out above, and to pay the fine (12,500.00 euros), so that the Public Prosecutor, Francesco Cajani, was then required to request the Judge to close the criminal case.
The legal implications of the case are described in the paper, in particular, the attorneys for Yahoo! Italia s.r.l. indicated to the Public Prosecutor's Office in Milan that the company would spontaneously conform to Decreto legislativo 30 maggio 2008, n. 109 (Legislative decree no. 109 dated 30 May 2008 : Transposition of 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 Communication Services or Public Communications Networks and Amending Directive 2002/58/EC) by storing log files for twelve months in future.

