CYBER FORENSICS E INDAGINI DIGITALI

Manuale tecnico-giuridico e casi pratici

CASI PRATICI

Estratto

G. Giappichelli Editore

INDICE DEI CASI PRATICI

a cura di *Francesco Cajani*

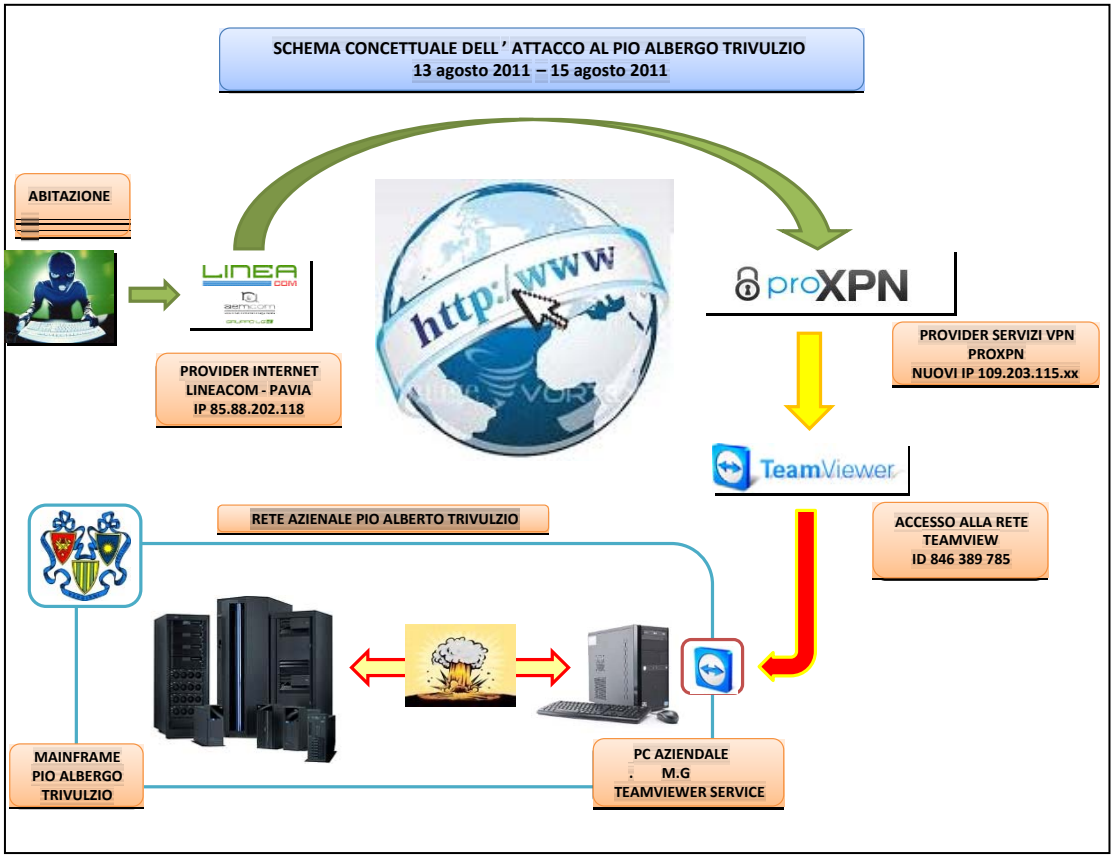
CASO PRATICO N. 5

Attacco informatico al Pio Albergo Trivulzio di Milano

a cura di F. CAJANI

Cap. 4 - LA RICEZIONE DELLA *NOTITIA CRIMINIS* E I PRIMI ATTI DI INDAGINE
Par. 11 – Furto di identità sul web

All'esito di una complessa indagine condotta dalla polizia postale di Milano, si è arrivati a ricostruire compiutamente il *modus operandi* utilizzato per porre in essere un sofisticato attacco informatico (qui sotto graficamente riassunto nel diagramma di flusso[1]) e, con esso, ad addivenire alla individuazione del relativo autore, per il quale veniva richiesta (e concessa dal g.i.p.) la misura cautelare del carcere.



Così sul punto l'ordinanza del tribunale di Milano che ha applicato la misura cautelare:[2]

[1] Agli atti dell'indagine e realizzati dalla polizia postale di Milano per una maggiore comprensione della vicenda.

[2] Ordinanza 8 novembre 2012 – est. Cantù Rajnoldi.

Sulla richiesta di data 5.10.2012 (depositata in data 9.10.2012) formulata dal Pubblico Ministero di applicazione della misura coercitiva della custodia cautelare in carcere per il seguente reato:

p. e p. dagli ***artt. 81, 61 n° 11, 615 ter commi 1, 2 e 3 c.p.*** perché, nella qualità di dipendente del Pio Albergo Trivulzio (PAT) e con abuso di relazione di ufficio, collegandosi – con la *user name* delfo2000@yahoo.it – ai servizi di anomizzazione di PROXPN attraverso l'IP 85.88.202.118 (assegnato staticamente al F. dalla società Lineacom Srl), ottenendo a suo favore l'assegnazione dei seguenti IP ad opera di PROXPN

collegamento	inizio	fine	
13 ago 2011	**16.37**	**16.37**	**213.179.212.76**
13 ago 2011	**16.45**	**16.46**	**213.179.212.76**
13 ago 2011	**16.47**	**17.30**	**213.179.212.76**
13 ago 2011	**19.09**	**21.37**	**109.203.115.89**
13 ago 2011	**22.45**	**02.31**	**109.203.115.71**
14 ago 2011	**02.39**	**03.02**	**213.179.212.122**
14 ago 2011	**03.05**	**03.29**	**173.231.157.74**
14 ago 2011	**03.42**	**04.23**	**109.203.115.66**
14 ago 2011	**19.33**	**20.51**	**109.203.115.109**
14 ago 2011	**21.11**	**21.42**	**109.203.115.109**
14 ago 2011	**22.10**	**22.11**	**213.179.212.70**
14 ago 2011	**23.47**	**23.47**	**213.179.212.69**
15 ago 2011	**01.38**	**01.47**	**173.0.5.51**

ed utilizzando il programma *Team Viewer,* accedeva abusivamente da remoto con ID 846389785 al sistema informatico del PAT protetto da misure di sicurezza.
Con le aggravanti che: dal fatto è derivato il danneggiamento di tale sistema informatico, l'interruzione parziale del suo funzionamento nonché la distruzione dei dati e delle informazioni ivi contenute; trattasi di sistema informatico relativo alla sanità pubblica e comunque di interesse pubblico.

In Milano dal 13 al 15 agosto 2011.

ORIGINE dell'INDAGINE
Il presente procedimento ha origine dal devastante[3] attacco informatico sferrato da anonimi *hacker* in prossimità del Ferragosto 2011 (le successive indagini hanno acclarato che detto attacco ha avuto inizio il 13.8.2011[4] alle ore 14.37 ed è proseguito fino alle 11.14 del 15.8.2011, giorno di Ferragosto) contro il sistema informatico del **PAT** (**Pio Albergo Trivulzio**), meglio noto ai cittadini milanesi come "BAGGINA" (dal nome del periferico quartiere in cui sorge dal lontano 1910) e formalmente e giuridicamente inserito nell'**Azienda di Servizi alla Persona – Istituti Milanesi Martinitt e Stelline e Pio Albergo Trivulzio** *(con sede a Milano in via Marostica n°8)*, ente pubblico senza scopo di lucro le cui finalità si realizzano precipuamente nei settori dell'assistenza socio-sanitaria.

Le **particolari modalità operative e temporali di detto attacco** (*il periodo ferragostano è notoriamente considerato periodo di complessiva e generale stasi delle attività lavorative e quindi ritenuto dagli autori di condotte illecite [spesso a torto come la presente vicenda dimostra] propizio per la commissione di reati in*

[3] In data 15.8.2011 M.G. (dipendente PAT con mansioni di amministratore di rete), dopo alcuni controlli operati per verificare alcuni malfunzionamenti denunciati da utenti esterni, si accorgeva (accedendo da remoto) che qualcuno aveva volutamente operato la **cancellazione di tutte le informazioni raccolte nel sistema, sia quelle inerenti la gestione amministrativa, sia quelle dell'attività sanitaria**. Emergeva in seguito che durante l'intrusione venivano **cancellate persino le copie di back-up e le password di accesso degli amministratori**.

[4] Va sottolineato che gli ignoti autori dell'attacco sembrano avere scelto con particolare cura il periodo temporale in cui sferrare l'attracco informatico, posto che il 13 agosto 2011 (giorno di inizio dell'attacco) cadeva di sabato, il 14.8.2011 di domenica ed il 15 (ferragosto e quindi giorno festivo per eccellenza) di lunedì.

considerazione dell'abbassamento del controllo sociale e dei maggiori intervalli temporali a disposizione per far perdere le proprie tracce) hanno fin da subito indirizzato gli inquirenti ad approfondire la conoscenza della **struttura interna del PAT deputata alla gestione di detto sistema informatico**, snodo nevralgico non solo per ciò che attiene all'organizzazione dei vari servizi socio assistenziali *(come detto in particolare la sede di via Trivulzio è storicamente destinata dal 1910 al ricovero ed all'assistenza di soggetti anziani totalmente o parzialmente non autosufficienti)*, ma anche alla gestione dell'ingente patrimonio immobiliare dell'ente *(frutto di lasciti di abbienti cittadini milanesi ed accresciuto considerevolmente con l'andare del tempo)* e dei collegati appalti per la relativa manutenzione e valorizzazione.

Le **indagini** condotte fin da subito (sul punto si evidenzia che già in data 18.8.2011 il PM di turno sentiva a s.i.t. G.E. – direttore dei sistemi informativi del PAT – che aveva sporto denuncia contro ignoti in data 17.8.2011 presso la Polizia di Stato – Compartimento Polizia Postale e delle Comunicazioni per la Lombardia – in seguito alla rilevata intrusione nella rete informatica aziendale) dalla **Polizia Postale di Milano** sotto la direzione ed il coordinamento della **Procura della Repubblica di Milano** sono consistite inizialmente nell'**assunzione a s.i.t.** dei vari soggetti[5] a vario titolo coinvolti nella gestione di detto sistema informatico e nel **sequestro** in data 18.8.2011 della **postazione informatica[6]** di M.G. (dalla quale sembrava essere partita l'intrusione), nonché di un secondo computer utilizzato dalla squadra tecnica del PAT come *file server* (ossia come *repository* di *file*), e nella **conseguente analisi forense degli stessi HD**, per poi proseguire in data 6.9.2011 nell'**acquisizione di documentazione** inerente l'organizzazione complessiva del servizio informatico del PAT.

LA RICHIESTA del PM

La richiesta cautelare del PM – condivisa da questo Giudice – ripercorre in modo dettagliato e puntuale le risultanze delle indagini.

I fatti assai articolati e complessi recepiti nell'incolpazione preliminare sono emersi a seguito di meticolose e febbrili indagini (**sul punto si evidenzia che alcuni passaggi cruciali per l'identificazione dell'autore di detto attacco informatico sono stati risolti tramite assistenza rogatoriale e con la decisiva cooperazione internazionale tra le forze di Polizia**) condotte con sapienza e notevole acume investigativo dalla Polizia Postale di Milano sotto la direzione della Procura della Repubblica di Milano.

Appare opportuno iniziare la trattazione dagli aspetti oggettivi di questa vicenda, riportando di seguito – **nei passaggi salienti e con caratteri grafici diversi** – la richiesta del PM, avendone positivamente riscontrato la puntuale conformità rispetto agli atti di indagine allegati.

In data 17 agosto 2011 la Polizia Postale di Milano trasmetteva al PM di turno la CNR nella quale si dava atto che:

Nella mattinata odierna, G.E.[7], direttore dei sistemi informativi del Pio albergo Trivulzio di Milano, ha presentato presso questo Compartimento una denuncia contro ignoti in seguito all'intrusione nella rete aziendale del PAT avvenuta – si suppone – nel corso del fine settimana antecedente Ferragosto. Esattamente quel giorno, dopo alcuni controlli operati per verificare alcuni malfunzionamenti denunciati da utenti esterni, un amministratore di rete dell'azienda[8] si accorgeva, accedendo da remoto, che ***qualcuno aveva volutamente operato la cancellazione di tutte le informazioni raccolte nel sistema, sia quelle inerenti la gestione amministrativa, sia quelli dell'attività sanitaria****. Addirittura, durante l'intrusione sarebbero stati cancellate perfino le copie di back-up e le password di accesso degli amministratori.*

[5] G.E. (direttore dei sistemi informativi del PAT) in data 18.8.2011, D.P. (responsabile organizzativo dell'Ufficio sistemi informativi del PAT) in data 18.8.2011, M.G. (amministratore di rete dell'azienda e primo ad accorgersi da remoto in data 15.8.2011 dell'attacco informatico) in data 14.9.2011 ed in data 26.9.2011, B.P. (dipendente della L. Service, società erogante in outsourcing servizi di configurazione e di assistenza sulla rete informatica dello stesso PAT all'epoca dei fatti oggetto di indagine) in data 18.8.2011 ed in data 14.9.2011 ed infine J.G.A. (componente del team informatico del PAT) in data 14.9.2011.

[6] Hard Disk SEAGATE con seriale SVYA6E21 del taglio di 250 Gb rimosso da un PC assemblato di colore nero con matricola 39100721010786.

[7] Cfr. anche dichiarazioni rese al PM in data 18.8.2011 ore 16.00 dallo stesso, il quale – dopo aver dichiarato che gli sembrava trattarsi "più di un brutto dispetto da parte di qualcuno che conosca bene il sistema e che ha avuto dei problemi lavorativi con il Trivulzio" – all'esito produceva **una lista dei soggetti che "rientrano nella categoria sopra indicata" (tra i quali vi era anche F.G.**).

[8] Trattasi di M.G.: cfr. le sue dichiarazioni allegate alla nota del 23 settembre 2011 e 29 settembre 2011.

Allo stato[9]*,* ***le uniche tracce rilevate dai tecnici del Trivulzio sono state una serie di connessioni registrate*** *durante la giornata di domenica 14* ***dal computer di M.G.****, uno dei tre amministratori di rete interni, lo stesso che si è accorto dell'attacco lunedì mattina. Il M. aveva lasciato l'ufficio venerdì 12 e sarebbe andato in vacanza a partire da martedì 16, quando gli altri due suoi colleghi avessero fatto rientro in ufficio. Il rappresentate dell'azienda ha comunicato che la macchina del M. è già stata separata dalla rete, a disposizione per gli opportuni controlli. Il direttore dei sistemi informativi ha pure precisato di aver già preso contatti con l'assistenza del software adoperato dal PAT al quale è stata delegata anche tutta la registrazione degli accessi alla loro rete per avere conferma della funzionalità del sistema*

Si procedeva quindi [10] al sequestro della postazione informatica del M. (dalla quale sembrava essere partita l'intrusione) nonché di un secondo computer utilizzato dalla squadra tecnica del PAT come *file server* (ossia come *repository* di *file* [11]).
Dal momento **che emergeva fin da subito come la macchina del M. (lasciata volutamente accesa dal medesimo per questioni tecniche [12]) potesse essere stata indebitamente utilizzata da terzi – tramite connessioni da remoto** [13] **– per consentire l'accesso alla rete del Pio Albergo Trivulzio** (PAT), si procedeva ad acquisizione dei *file* di *log* relativi agli indirizzi IP [14] del sistema *TeamViewer* (software che permette di controllare qualunque personal computer da remoto attivando funzionalità di condivisione del *desktop* e trasferimento dei *file* [15]) tra le ore 14.00 di venerdì 12 agosto e le ore 14.00 del successivo lunedì 15.

La PG delegata procedeva altresì, nella giornata del 22 agosto 2011 [16], ad una verifica in loco delle macchine compromesse del PAT ed in particolare del cosiddetto "NAS1", computer di *file sharing* (ossia: condivisione dei *file*) dal quale sono stati cancellati tutti i volumi dati nonché – previa autorizzazione del PM *ex* art. 360 c.p.p – alla analisi delle stesse[17] al fine di rinvenire tracce utili all'identificazione dell'agente: emergeva così, in particolare, come verso tale macchina "NAS1" **sia stata lanciata una procedura di *teracopy*[18] il 13.8.2011, non andata a buon fine per motivi sconosciuti**.

Con decreto del PM del 6 settembre 2011 veniva altresì acquisita presso il PAT documentazione potenzialmente utile al fine di ricostruire un ipotetico movente delle vicenda (ove, come poi successivamente riscontrato, la stessa potesse collocarsi nell'ambito dei rapporti interni allo stesso PAT) e, in particolare:

- *"Documento Programmatico per la Sicurezza" di cui al D.lgs 196/2003;*
- *elenco del personale assunto, con i relativi dati identificativi di ciascuno di essi e la data di assunzione, a partire dal 2009;*

---

[9] Cfr. cronologia eventi prodotta da G.E. al PM in data 18.8.2011 ed effettuata dalla L. Service.

[10] Cfr. nota del 19 agosto 2011.

[11] Il termine file server si riferisce generalmente ad una macchina progettata per mettere a disposizione degli utilizzatori di una rete di computer dello spazio su un disco (disco singolo o composto da più dischi) nel quale sia possibile salvare, leggere, modificare, creare file e cartelle condivise da tutti, secondo regole o autorizzazioni che generalmente il gestore di rete organizza e gestisce.

[12] Cfr. sit M. del 14.9.2011: "alcune volte mi scordavo la macchina accesa, nel caso di ferragosto l'ho tenuto acceso perché E.G., mio collega del Team Informatico, a fine pranzo di quel venerdì mi chiese di tenere aperta la sessione di ENCO che è il programma della contabilità grafica che risiede sul server Ercole". Sulla possibilità di utilizzo della sessione di ENCO da parte del F. vedi infra.

[13] Cfr. denuncia di G.E.: "sebbene gli attacchi informatici subiti, siano iniziati sabato 13, e siano durati tutto il fine settimana, abbiamo rilevato unicamente quelli avvenuti nella giornata di domenica … Abbiamo contattato il servizio di assistenza del programma "TeamViewer", che utilizziamo per controllare da remoto le macchine informatiche, gli addetti ci hanno confermato che è possibile risalire agli I.P. delle connessioni avvenute …".

[14] Un Indirizzo IP è un numero che identifica univocamente nell'ambito di una singola rete i dispositivi collegati con una rete informatica che utilizza lo standard IP (Internet Protocol). Ciascun dispositivo (router, computer, server di rete, stampanti, alcuni tipi di telefoni, ...) ha, quindi, il suo indirizzo. Semplificando, un indirizzo IP può essere visto come l'equivalente di un indirizzo stradale o un numero telefonico dei dispositivi collegati su internet. Infatti, così come un indirizzo stradale o un numero telefonico identifica un edificio o un telefono, così un indirizzo IP identifica univocamente uno specifico computer o un qualsiasi altro dispositivo di rete o una rete. A sua volta, in una rete possono essere utilizzati altri indirizzi IP validi localmente analogamente alla numerazione degli interni di un edificio": cfr. *http://it.wikipedia.org/wiki/Indirizzo_IP*. Gli indirizzi sono composti da 4 byte, una parte dei quali identificano la rete e la restante parte il nodo all'interno della rete. Ogni byte è separato dagli altri con un punto e per questo gli indirizzi IP hanno una struttura di questo tipo: 194.21.28.40. L'assegnazione dei numeri IP viene effettuata dall'ICANN, un ente americano che li distribuisce, singolarmente o in blocco, ai richiedenti.

[15] Cfr. *www.teamviewer.com/it/index.aspx.*

[16] Cfr. nota del 23 agosto 2011.

[17] Cfr. nota del 6 settembre 2011.

[18] Trattasi di programma utilizzato per copiare grosse quantità di dati.

- *contratto di collaborazione in essere dal 2002 al febbraio 2010 con il consulente informatico C.C.[19];*
- *contratto di collaborazione in essere dal 1998 al dicembre 2005 con il consulente informatico A.C.[20];*
- *contestazioni effettuate a carico dell'ex dipendente dei Sistemi Informativi F.A.[21] dal giugno 2009 al ottobre 2010 nonché di quelle eventualmente effettuate a carico dell'ex dipendente dei Sistemi Informativi F.G[22] dal 2004 al novembre 2006; documentazione relativa alle mansioni concretamente svolte dai due suddetti ex dipendenti;*
- *contestazioni disciplinari a carico di C.A.[23], nonché di altri dipendenti/collaboratori a partire dal 2009 ad oggi;*
- *contratto di collaborazione attualmente in essere con la società LAN service [24];*
- *contratti relativi all'acquisto di forniture hardware/software a partire dal 2009 nonché delle eventuali consulenze informatiche con soggetti o società terze in essere con l'Istituto disposte a partire dal 2009 e/o ancora in essere alla data di notifica del presente provvedimento*
- *relazioni tecniche interne attinenti agli accessi a sistemi informatici del PAT non autorizzati, avvenuti nel gennaio 2006, nel ottobre 2010 e nel maggio/giugno 2011 (così come indicati dal dott. G. al PM in data 18.8.2011);*
- *relazioni tecniche interne relative all'attacco informatico denunciato il 17.8.2011, comprensiva di eventuali relazioni sulle attività di recupero dei dati informatici presenti nei sistemi compressi;*

Venivano successivamente acquisiti [25] anche gli *hard disk* del sistema informatico del PAT relativi alla macchina denominata "PRESENZA-MACS", che concentrava l'insieme delle timbrature, cioè i dati di rilevazione e controllo delle presenze lavorative giornaliere all'interno dell'azienda (dal momento che B.P. della L. Service aveva riferito che, nei giorni successivi l'attacco, aveva notato da parte di quella macchina un elevato numero di connessioni potenzialmente sospette).

Con nota del 29 settembre 2011 la PG restituiva **l'analisi forense degli HD sequestrati il 18 agosto scorso, ed in particolare del computer in uso a M.** (dal quale si ritiene sia avvenuta l'intrusione), analisi che confermava come

l'attacco sarebbe avvenuto dal PC del M. (PATHD02), utilizzando il programma *Team viewer*, con l'ID 846389785;
l'intrusione è iniziata nel primo pomeriggio del 13 agosto (dalle ore 14.37), protraendosi almeno sino alle 11.14 di Ferragosto;
l'intruso possedeva probabilmente la *password* di accesso mancando tracce su altre modalità di accesso al sistema;
l'intruso ha cercato di nascondere le tracce dell'attacco cancellando il log di *Team Viewer* con la modalità "salva", cioè aprendo il *file* di *log*, cancellando quanto vi era memorizzato e poi salvando il file vuoto.

[…]

Queste dunque le conclusioni della Polizia Postale, compendiate nella nota del 21 settembre 2012, sui primi accertamenti di PG così come finora descritti:

Le investigazioni avviate da questo Compartimento sin dall'immediatezza la mattina del 17 agosto 2011, cioè nel momento in cui G.E., all'epoca responsabile dei Sistemi informatici del PAT, denunciò il fatto, non solo contribuirono a confermare l'iniziale ipotesi che la distruzione del sistema era stata causata da un attacco all'infrastruttura informatica dell'azienda proveniente dall'esterno, ma permisero di realizzare soprattutto un disegno della trama tecnica (modalità di accesso al sistema, cancellazione dei dati di memoria e successiva – conclusiva – sovrascrittura delle tracce informatiche della intrusione – tentativo di copiatura) con cui questo attacco era stato realizzato. I contenuti delle relazioni realizzate dal personale di questo Compartimento del 29 settembre e del 25 ottobre 2011 sintetizzano l'ordito di questa trama e sono essenziali sia alla sua esatta comprensione sia per quanto riguarda i rilievi successivi fino all'identificazione finale del responsabile.

[19] Trattasi di nominativo emerso dalla lista depositata da G. il 18.8.2011.

[20] Trattasi di nominativo emerso dalla lista depositata da G. il 18.8.2011.

[21] Trattasi di nominativo emerso dalla lista depositata da G. il 18.8.2011.

[22] Trattasi, come già ricordato, di nominativo emerso dalla lista depositata da G. il 18.8.2011 ed in relazione al quale inizialmente non erano emerse, dal racconto riferito da G., contestazioni disciplinari effettuate allo stesso.

[23] Trattasi di nominativo emerso dalla lista depositata da G. il 18.8.2011.

[24] Trattasi della società che forniva assistenza informatica al PAT all'epoca dei fatti.

[25] Cfr. nota del 23 settembre 2011.

Ascoltate le persone che potevano fornire elementi utili a ricostruire il quadro della organizzazione generale del PAT e i dettagli sui momenti prossimi alla scoperta del fatto, in particolare gli appartenenti al gruppo di gestione informatica (fra i quali non vi era F.), visionato direttamente tutti i luoghi interessati dalla vicenda – in specie quelli ove erano fisicamente allocati server e computer – verificato quindi lo stato dell'infrastruttura informatica e le modalità con le quali quest'ultima era stata annichilita, gli operatori di questo Compartimento accertavano l'inesistenza di una qualsiasi traccia di natura classica. L'attacco al sistema informatico del PAT era stato infatti realizzato esclusivamente per mezzo di vie telematiche e quello era l'unico cammino sul quale poteva forse trovarsi qualche elemento utile.
Il problema inizialmente emerso era che prima di uscire dal sistema l'autore dell'azione criminosa, dimostrandosi accorto, astuto e soprattutto preparato, si era premurato di cancellare anche le tracce informatiche del suo accesso abusivo allorché si allontanava dall'infrastruttura del PAT. Queste tracce sarebbero state le "impronte" lasciate dal suo passaggio e solo queste avrebbero potuto in qualche modo tradirlo. Di qui la cancellazione, non solo dei dati, ma anche la distruzione parziale del sistema, per renderlo inagibile ed evitare che una sua ricomposizione potesse far emergere queste "impronte".
A parere di questo Compartimento, la modifica non necessaria di un file di log degli accessi da esterno (il registro informatico degli accessi) che erano stati effettuati con il programma "team viewer", si spiega con la necessità di sviare la ricostruzione degli stessi accessi. Un esperto del settore sa che la mera cancellazione del file sarebbe stata insufficiente perché una normale analisi tecnica lo avrebbe potuto recuperare. La modifica del file, ad esempio con la riscrittura del suo contenuto, in caso di recupero avrebbe potuto portare gli investigatori sulla "strada sbagliata".
A tali fini, non è da sottacere la circostanza che l'analisi tecnica dell'azienda L. Service (che aveva all'epoca un contratto di assistenza con il PAT) a seguito del suo intervento in modalità IRT (incident response team) dopo l'attacco informatico, non rivelò dati utili per le indagini.
Ciononostante, di fronte all'impossibilità di seguire in quel momento strade diverse dall'indagine informatica, questo Compartimento avviava una serie di complesse e laboriose analisi tecniche su diverse componenti dell'infrastruttura informatica.
L'idea era stata quella di ***provare a ricomporre la configurazione degli hard disk che costituivano l'ossatura dell'infrastruttura, cioè ricostruire le memorie informatiche del PAT compromesse dall'attacco per potervi poi ricercare eventuali tracce estranee alla normale conduzione aziendale, riconducibili cioè all'attacco****. In altre parole restaurato il tracciamento delle operazioni informatiche giornalmente condotte nel sistema informatico nel PAT si sperava di poter isolare e identificare così una traccia riferibile all'intrusione esterna con la quale è stato sferrato l'attacco (cfr. Informativa di questo Compartimento del 23-09-2011 e successivamente Relazione del 29-09-2011)".*

[…]

Così ancora l'annotazione della Polizia Postale del 21 settembre 2012:

Lo studio di questa catena di eventi ha permesso di giungere agli IP ed agli account di F., realizzando quindi una sorta di chiusura del cerchio che si è conclusa ritornando al punto di origine, un dipendente dell'azienda, già oggetto di procedimento disciplinare e che parrebbe aver avuto motivi di risentimento nei confronti almeno di un suo dirigente (cfr note già trasmesse e sommarie informazioni rese al PM da G.).
Come già comunicato, ***il principale risultato della complessa analisi condotta sugli hard disk del PAT fu la scoperta che per accedere all'infrastruttura informatica l'ignoto attaccante era "transitato" attraverso il computer di M.G.****, uno dei tecnici impiegati presso l'azienda pubblica col compito di gestire la manutenzione del sistema informatico. In quanto tale, M. era (è) in possesso di tutti i privilegi di amministratore, quindi di tutte le password.*
M. era anche il tecnico che aveva segnalato per primo l'attacco, poco dopo le undici del mattino di Ferragosto, accortosi della scomparsa di tutti server virtuali dall'infrastruttura virtuale, dopo essersi collegato da remoto col suo computer personale per una verifica di routine.
In partenza per le vacanze estive, ***il pomeriggio del 12 agosto M. se ne era andato dall'ufficio lasciando il suo computer acceso.*** *Era stato lui stesso a raccontarlo durante la sua prima escussione a sommarie informazioni il 14 settembre 2011 in rientro dalle ferie: glielo aveva chiesto un collega impiegato come analista (addetto alla statistiche) G.E.,* ***in modo da lasciare disponibile la sessione del programma "ENCO", un software destinato alla gestione della contabilità aziendale interna dell'istituto installato dai tecnici dell'azienda, fra i quali lo stesso F., come emerge dalla dichiarazione difensiva che questi aveva presentato nel corso del procedimento disciplinare a suo carico.***
Lasciare aperto il collegamento con la Rete era un'abitudine consolidata che consentiva a M. di intervenire anche da remoto in caso di problemi al sistema. Infatti la mattina di Ferragosto si era collegato dopo che alcuni settori della struttura sanitaria avevano segnalato anomalie di funzionamento fin dal giorno prima. L'intrusione era già cominciata il 13 e probabilmente l'attaccante aveva iniziato a cancellare i server virtuali.

Come già indicato, per entrare nella infrastruttura l'attaccante aveva utilizzato il software noto col nome di Team Viewer, un programma attraverso il quale chiunque può instaurare attraverso Internet un collegamento per controllare il proprio computer a distanza operando da un altro computer ubicato in qualunque parte del mondo, come se invece si trovasse davanti al suo. Si tratta dello stesso software adoperato da M. per lavorare da remoto. Questo software risulta diffuso fra circa un centinaio di milioni di utenti ed è quindi utilizzato su scala globale per finalità lecite trattandosi di un mezzo di utilità per persone e imprese.
L'installazione di Team Viewer sul personal computer di M. era, per stessa ammissione dell'interessato, un fatto universalmente noto. Lo utilizzavamo perfino dei fornitori esterni che così si collegavano alla Rete dopo avergli chiesto l'accesso. Una gestione per così dire molto "familiare" dell'infrastruttura come si può evincere – ci troviamo sempre innanzi alle ammissione del tecnico – anche dalla password utilizzata: semplicemente «trivulzio», quella forse adoperata anche dall'attaccante per accedere prima al computer di M. e poi all'intera Rete aziendale. Da tenere in conto pure che M., peraltro, aveva conservato su almeno uno dei computer coi quali lavorava in rete anche un file con l'intero elenco delle password di accesso ai tutti sistemi informatici del PAT, con esclusione della password del server per i dati sanitari, che infatti non sono stati cancellati durante l'attacco.
Accedere alla postazione di M. significava quindi avere la chiave di accesso a tutti i varchi del sistema, per le varie macchine fisiche e virtuali componenti dell'infrastruttura, raggiungibili attraverso una semplice connessione RDP (Remote Desktop Control), un protocollo Microsoft incluso nei pacchetti commercializzati dall'azienda americana. Si tratta di un servizio che quando viene attivato permette di accedere alle risorse di qualsiasi macchina dopo essere entrati nel computer principale al quale la prima risulta collegata, nel caso di specie quello di M., dalla quale lui era abituato a controllare i server aziendali.

Come già ricordato, con nota del 29 settembre 2011 la Polizia Postale comunicava di aver trovato la **traccia di un collegamento *Team Viewer*, un ID identificato dalla stringa numerica «846389785».** Paradossalmente, poiché l'analisi tecnica condotta aveva rivelato che l'attaccante si era dato da fare per cancellare oltre ai contenuti anche ogni traccia dell'attacco, sovrascrivendo anche i *log* del suo accesso in modo da renderli irriconoscibili, questo ID veniva indicato come quella unica "impronta" dalla quale poter partire.
Nonostante l'ID Team Viewer «846389785» fosse collegato ad una versione *free* del software, scaricabile anonimamente dalla Rete (e con possibilità di tracciamento, come già ricordato, del solo ultimo collegamento registrato), la omonima società che commercializza il software *Team Viewer* collaborava pienamente alle richieste della Autorità Giudiziaria rilasciando esaurienti chiarimenti a tutte le domande tecniche presentate dal personale della Polizia Postale di Milano: **si acquisiva così l'informazione secondo cui l'ID 846389785, rinvenuto a seguito di analisi tecnica quale traccia dell'attacco, alle ore 11:30 circa del 15.08.2011 era stato associato all'IP 109.203.115.70.**

[...]

Così sempre la nota di PG del 21 settembre 2012:

*A seguito di approfondimenti di routine, **si chiariva che tale IP era nella disponibilità della società olandese SolidHost, che fornisce servizi telematici.** Di seguito ai primi contatti internazionali, si rendeva necessaria una rogatoria verso l'Olanda, emessa […] il 16-12-2011 a seguito di richiesta di questo Compartimento del 15-12-2011.*
*Il 29.12.2011 si apprendeva dai canali di cooperazione di polizia che **il server al quale corrispondeva l'IP 109.203.115.70, oggetto di indagine, era in effetti allocato nel Regno Unito ove risultava di proprietà della britannica EUKHost, presso cui era stato preso in noleggio da SolidHost e pertanto era necessario acquisire i dati telematici nel Regno Unito**.*
La risposta formale delle Autorità olandesi riporta il processo verbale dal quale sostanzialmente emerge:
– che SolidHost fornisce servizi internet basati su server fisici e virtuali, controllati dalla stessa azienda (per conto dei clienti) o dai clienti stessi, che possono utilizzare i server per tutto ciò che vogliono sempre che sia in rispetto della legge o delle policy che sono disponibili a www.solidhost.com/aup . Nei casi in cui sono i clienti a gestire il server, SolidHost non vi ha diretto accesso;
– SolidHost ha la possibilità di sapere l'indirizzo IP dei clienti che richiedono servizi online. Nella maggior parte dei casi, se l'ammontare del pagamento è basso, effettua un breve check per verificare che la georeferenziazione dell'IP è compatibile con l'indirizzo di fatturazione e telefono fornito dal cliente. In caso positivo accetta l'ordine senza ulteriori dettagli. In caso di dubbio, o per pagamenti rilevanti, richiede ulteriore documentazione (come copia di foto identificativa etc.);
– che i clienti possono pagare con sistema Pay-Pal, carte di credito o bonifico bancario. SolidHost non è autorizzata a trattenere dettagli di carte di credito. Per i pagamenti con carta di credito utilizza un servizio esterno (www.2checkout.com) e quando un cliente vuole pagare con carta di credito è reindirizzato a questo sito verso cui paga, per essere nuovamente reindirizzato a SolidHost quando il pagamento è fatto. 2checkout

invia periodicamente le somme raccolte sul conto corrente di SolidHost sottraendo la commissione; pertanto non c'è visibilità sui numeri delle carte di credito. Quando il cliente paga con PayPal o bonifico bancario SolidHost non conserva l'ID e il numero di conto corrente o ID PayPal nel proprio database. I dati dei clienti e le fatture sono memorizzati in un database il cui accesso è riservato al solo personale di SolidHost oltre che agli stessi clienti attraverso il portale online;
– che SolidHost non detiene alcun dato. L'indirizzo IP è tenuto in un server a Londra che è stato preso a noleggio dal partner nel Regno Unito EUKHost e rivenduto al cliente come intero. In altre parole SolidHost è l'elemento di mezzo senza avere alcun accesso al server. I clienti pagano SolidHost che a sua volta paga EUKHost. Anche quando i clienti hanno dei problemi questi vengono girati ad EUKHost, SolidHost non ha alcun accesso fisico o virtuale al server.

Risultava pertanto necessaria una richiesta di assistenza giudiziaria verso le Autorità britanniche, per acquisire il traffico telematico relativo all'IP 109.203.115.70 nel periodo di tempo riferibile all'attacco, inviata per i canali di cooperazione di polizia, per la quale il 23 marzo 2012 l'Interpol britannico faceva sapere che era stata approvata dall'Autorità centrale ed assegnata alle forze di polizia (SOCA).
Si è scoperto quindi che ***i server di EUKHost sono di proprietà di altra società britannica PoundHost, verso la quale si sono svolte le attività di analisi degli esperti del SOCA.***
Le attività svolte nel Regno Unito hanno fatto comunque ritornare le indagini in Olanda.
Infatti le attività svolte unitamente al SOCA britannico hanno evidenziato che la catena degli eventi prevede un ulteriore passaggio: ***l'attaccante ha nascosto il suo IP utilizzando un servizio di anonimizzazione offerto online dalla società olandese PROXPN, che gli ha così consentito di presentarsi sulla Rete con IP diversi dal suo, tra i quali il 109.203.115.70.***

Più specificatamente e come ben evidenziato nella nota di PG del 3 agosto 2012**, dall'analisi ad opera del SOCA del *server* di PoundHost è emerso come al fine di collegarsi all'IP 109.203.115.70 l'utente avrebbe utilizzato il software della società PROXPN**[26] **che utilizza le macchine di EUKHost.**

[…]

Così sempre la nota della Polizia Postale del 21 settembre 2012:

In questa fase si coglie l'occasione per mettere in luce la preziosa collaborazione che la Cyber Crime Unit del SOCA ha prestato dopo essere stata incaricata di dare corso alle richieste di collaborazione per ***analizzare i server di EUKHost/PoundHost. Nel corso dell'analisi gli agenti hanno trovato non solo l'IP in questione ma anche altre serie di IP che iniziavano con 213 e 109, riconducibili proprio a PROXPN, cioè ad altri utilizzi, nel contesto di indagine, del servizio di anonimizzazione.***

Nel corso di queste attività operative, questo Compartimento veniva in contatto col ***il referente tecnico di PROXPN in Olanda****[27], che il 6 agosto u.s., rispondendo alla richiesta di questo Ufficio****, ha inviato la lista integrale degli utenti che avevano utilizzato il servizio VPN dalla macchina inglese sotto analisi (per gli indirizzi IP con classe 109.203.115 a partire da 001) per il periodo compreso tra il 12 ed il 15 di agosto 2011, cioè i giorni comprendenti l'attacco oggetto di indagine.***

La lista contiene tutti gli IP di PROXPN utilizzati su scala globale che in quei giorni si erano connessi al server di EUKHost sfruttando i servizi di anonimizzazione. Da questa lista questo Compartimento ha estrapolato quelli riferibili ad utenti italiani (per classi di IP, userID e provider di servizi di posta elettronica) come già segnalato il 7 agosto[28] ai fini della richiesta di decreto per l'identificazione degli account e per l'acquisizione del traffico telematico.
Nelle more dell'acquisizione di questi dati, emergeva altresì che uno degli account di posta elettronica di registrazione contenuti nella citata lista, quello denominato xxxxx@yahoo.it, risultava riferibile alla persona di F.G., quale suo contatto e-mail utilizzato pubblicamente sul web[29].

[26] Sui collegamenti tra PROXPN e SolidHost cfr. sempre la nota del 3 agosto 2012: "Vi è il sospetto che PROXPN sia strettamente collegata (in senso societario) con SolidHost, in un rapporto non solo meramente commerciale come emergeva dall'esito della prima rogatoria effettuata in Olanda. Ciò emerge sviluppando con whois domain database il sito web di proxpn.org che riporta il collegamento proprio con SolidHost".

[27] BALL Kent, n.m.i.

[28] Cfr. nota agli atti avente pari data.

[29] Vedi all. 2 alla nota del 7 agosto 2012.

Come evidenziato nella relazione allegata, le connessioni di xxxxx@yahoo.it registrate da PROXPN sono le uniche compatibili sia con l'intero periodo dell'attacco, che si presume realizzato tra il 13 e il 15 agosto 2011, sia con le singole connessioni remote effettuate sul computer di M.

Grazie a questa ricostruzione, rileggendo i dati recuperati dalle macchine attaccate con i nuovi elementi raccolti in campo internazionale, **gli operatori di PG sono riusciti a scoprire ulteriori sessioni di accesso remoto effettuate dal numero ID *Team Viewer* «846389785» riconducendo a questo ID tutti gli attacchi effettuati sia tramite l'IP della classe 109.203.115.xx sia tramite gli altri IP utilizzati per coprire la provenienza e ricevuti da PROXPN.**

Nella seguente tabella indicata dalla Polizia Postale nella nota del 21 settembre 2012, si riportano le specifiche delle singole sessioni, ritrovate nell'*hard disk* del Pio albergo Trivulzio in uso a M.[30] a seguito della ricezione dell'elenco degli IP connessi con l'ID di *Team Viewer* (riferiti all'attacco):

collegamento	inizio	fine	
13 ago 2011	16.37	16.37	**213.179.212.76**
13 ago 2011	16.45	16.46	**213.179.212.76**
13 ago 2011	16.47	17.30	**213.179.212.76**
13 ago 2011	19.09	21.37	**109.203.115.89**
13 ago 2011	22.45	02.31	**109.203.115.71**
14 ago 2011	02.39	03.02	**213.179.212.122**
14 ago 2011	03.05	03.29	**173.231.157.74**
14 ago 2011	03.42	04.23	**109.203.115.66**
14 ago 2011	19.33	20.51	**109.203.115.109**
14 ago 2011	21.11	21.42	**109.203.115.109**
14 ago 2011	22.10	22.11	**213.179.212.70**
14 ago 2011	23.47	23.47	**213.179.212.69**
15 ago 2011	01.38	01.47	**173.0.5.51**

Di seguito, la tabella sintetica delle connessioni realizzate dall'*account* di F. durante quell'operazione (gli orari sono ancora quelli americani):

	INIZIO connessione		FINE connessione		
xxxxx@yahoo.it	13 ago 2011	08:27	13 ago 2011	10:16	85.88.202.118
xxxxx@yahoo.it	13 ago 2011	13:09	13 ago 2011	15:37	85.88.202.118
xxxxx@yahoo.it	13 ago 2011	16:44	13 ago 2011	20:31	85.88.202.118
xxxxx@yahoo.it	13 ago 2011	21:02	13 ago 2011	21:04	85.88.202.118
xxxxx@yahoo.it	13 ago 2011	21:41	13 ago 2011	22:24	85.88.202.118
xxxxx@yahoo.it	14 ago 2011	05:08	14 ago 2011	05:11	85.88.202.118
xxxxx@yahoo.it	14 ago 2011	05:35	14 ago 2011	06:36	85.88.202.118
xxxxx@yahoo.it	14 ago 2011	08:05	14 ago 2011	09:43	85.88.202.118
xxxxx@yahoo.it	14 ago 2011	13:31	14 ago 2011	15:58	85.88.202.118
xxxxx@yahoo.it	15 ago 2011	05:32	15 ago 2011	05:43	85.88.202.118
xxxxx@yahoo.it	15 ago 2011	17:15	15 ago 2011	17:22	85.88.202.118

[30] Cfr. annotazione di PG del 29.9.2011 in relazione all'HD identificato come PATHD02 (all'interno del quale la PG ha ritrovato il log del programma Team Viewer).

Il confronto delle sole connessioni attuate con indirizzi di classe IP 109.203.115 ricavate dal recupero dei dati appena menzionato nell'*hard disk* del Trivulzio in uso a M. con la lista di connessioni fornite da PROXPN relativamente all'*account xxxxx@yahoo.it* conduce alla seguente ultima tabella:

	Orario connessioni al servizio *VPN* (*account* xxxxx@yahoo.it)		**Orario connessioni con *Team Viewer*** (recupero dati dell'analisi al PAT)		
Data	**Inizio**	**Fine**	**Inizio**	**Fine**	**IP *(di copertura)***
13 ago 2011	**19:09**	**21:37**	**19.09**	**21.37**	109.203.115.89
13 ago 2011	**22:44**	**02:31**	**22.45**	**02.31**	109.203.115.71
14 ago 2011	**03:41**	**04:24**	**03.42**	**04.23**	109.203.115.66
14 ago 2011	**11:08**	**11:11**	**11.10**	**11.10**	109.203.115.95
14 ago 2011	**11:35**	**12:36**	**11.42**	**12.16**	109.203.115.80
14 ago 2011	**19:31**	**21:58**	**19.33**	**21.42**	109.203.115.109

Come ben indicato dalla Polizia Postale sempre nella nota del 21 settembre 2012, **questa assoluta coincidenza dei collegamenti temporali riscontrati in due situazioni diverse, gli uni provenienti dalle registrazioni dei *log* olandesi di PROXPN, gli altri dai dati presenti nell'*hard disk* del PAT recuperato ed in uso al M., riaggregati ed analizzati alla luce delle ultimissime risultanze, dimostra in maniera inequivocabile che l'utilizzatore della casella di posta elettronica *xxxxx@yahoo.it*, collegatosi ai servizi di PROXPN attraverso l'*IP* 85.88.202.118, è certamente l'attaccante che – previo accesso abusivo – ha danneggiato il sistema informatico del Pio albergo Trivulzio operando durante i giorni 13, 14 e 15 agosto 2011**.

Come indicato dalla Polizia Postale[31], **l'IP 85.88.202.118 rientra in un *range* di otto indirizzi che F. ha in affitto, fin dal 2007, da Lineacom Srl, società di servizi informatici del Comune di Pavia.** Non è chiaro lo scopo al quale questi indirizzi telematici siano destinati ma sembrerebbero in qualche modo rivolti ad una sorta di *web hosting* sebbene le verifiche in Rete non hanno potuto riscontrare con certezza l'esistenza di questa pratica commerciale.

Il responsabile di Lineacom Srl ha riferito di non possedere il traffico telematico dell'IP 85.88.202.118 trattandosi di IP fisso stabilmente assegnato all'utente. Le connessioni a PROXPN effettuate da F. potrebbero pertanto eventualmente emergere a seguito di analisi dei suoi computer ma va comunque evidenziato **un ulteriore elemento di assoluta importanza** nel quadro accusatorio: a seguito dell'acquisizione dei *files* di *log* presso il gestore "*yahoo*" risulta che tra il 25 e il 28 agosto 2011 e tra il 19 e il 21 novembre 2011 F.G. ha consultato la casella di posta elettronica xxxxx@yahoo.it anche passando proprio per i servizi di PROXPN.

GRAVI INDIZI di COLPEVOLEZZA

Gli elementi raccolti dall'Ufficio del PM e sopra illustrati nella loro progressiva sequenza temporale e concatenazione logica denotano **un pregnante quadro indiziario a carico dell'indagato F.G.** quale autore del contestato accesso abusivo da remoto con ID 846389785 al sistema informatico del PAT protetto da misure di sicurezza.

Detti elementi si desumono in particolare dalle sopra citate **informative[32] della Polizia di Stato – Compartimento Polizia Postale e delle Comunicazioni per la Lombardia** – riepilogative delle complesse indagine tecniche condotte fin dal 17.8.2011 (data della denuncia contro ignoti sporta da G.E., direttore dei sistemi informativi del PAT) ed ininterrottamente (in un **complicato dedalo informatico percorso a ritroso** grazie al prezioso ***filo d'Arianna*** costituito dall'unica individuata **traccia lasciata in occasione dell'attacco informatico**) fino alla recente individuazione di F.G., quale autore dell'accesso abusivo alla rete informatica del PAT di data 13 – 15.8.2011.

[31] Cfr. nota del 17.8.2012.

[32] Vedi in particolare quelle di data 21.9.2012 – 29.9.2011 – 3.8.2012 e 17.8.2012.

Detta traccia è costituita dall'**ultimo *log* dell'accesso remoto di data 15.8.2011** la cui analisi ha consentito di affermare che l'intrusione è stata realizzata per mezzo di ***"Team Viewer"***, particolare *software* utilizzato per accedere e controllare altri computer da remoto attraverso codici di accesso.

La compagnia tedesca proprietaria di questo software ("Team Viewer"), su richiesta della Polizia italiana, ha decifrato il proprio *log* rivelando che quell'accesso era giunto dall'**indirizzo IP 109.203.115.70** risultato appartenere a **EUkHost**, una **società britannica che fornisce servizi web acquistabili direttamente dal suo sito in Rete**. A seguito della prima richiesta rogatoriale, la Polizia britannica informava questo Ufficio che **EUkHost aveva affittato l'IP 109.203.115.70 a SolidHost, azienda olandese di Rotterdam**.

Successivi accertamenti effettuati in via di cooperazione internazionale confermavano che detta società olandese (SolidHost) aveva affittato l'IP 109.203.115.70 da EUKHost. Peraltro emergeva che **i relativi *server* si trovavano nel Regno Unito** con la conseguente impossibilità per SolidHost di procedere al controllo o alla copia dei dati presenti nell'archivio informatico per la ricerca dei log attinenti le investigazioni.

Il SOCA britannico, avuto accesso ad EUKHost, identificava un'**altra azienda, materiale proprietaria del *server*** (**PoundHost**, ubicata in Gran Bretagna) ed otteneva un nuovo mandato dalla Pubblica accusa allo scopo di ricevere informazioni da questa ulteriore azienda. Questa attività tecnica ha alla fine ricondotto le investigazioni verso i Paesi Bassi.

Al termine di queste attività condotte in collaborazione con il SOCA, è stato scoperto che l'**indirizzo IP 109.203.115.70 formalmente appartenente a EUKHost, in realtà è stato noleggiato a SolidHost ma è gestito da PROXPN**, **azienda olandese che offre servizi internet** (per esempio nascondere gli indirizzi IP di provenienza dei propri clienti) contattatabile on-line (www.proxpn.com).

Esistono alter tre indirizzi IP riguardanti PROXPN (sebbene appartenenti a SolidHost) utili per le investigazioni, indirizzi adoperati per l'attività criminosa e rintracciati in un computer delle vittime dopo un'analisi tecnica:

213.179.212.xxx 173.0.5.xxx 173.231.157.xxx

Deve quindi convenirsi con quanto affermato dal PM e cioè che **gli autori del crimine si sono collegati a PROXPN per scaricare il programma offerto on-line da questa azienda grazie al quale hanno avuto poi l'opportunità di nascondere il loro IP originale ricevendo un temporaneo IP "pulito"** (compreso nella serie 109.203.115.xxx, 213.179.212.xxx, 173.0.5.xxx, 173.231.157.xxx), dopodiché – utilizzando questo IP coperto – hanno realizzato l'attacco criminale alla rete informatica del PAT ed ai relativi archivi elettronici. Il meccanismo trova sostanziale conferma dalla perfetta sequenza cronologica degli avvenimenti e delle connessioni rinvenute nel computer dell'azienda.

Successivamente veniva **acquisito da PROXPN** (grazie alla cooperazione internazionale condotta unitamente al SOCA britannico ed alla polizia olandese) un **dettagliato elenco riportante i dati del traffico telematico in entrata sull'IP 109.203.115.70 di PROXPN tra il 12 ed il 15.8.2011**.

Dalla disamina delle connessioni ivi elencate emergevano anche ripetuti collegamenti (nelle tre giornate di interesse: 13, 14 e 15 agosto 2011) da parte di alcuni utenti che per denominazione (sabatini.ruby@gmail.com – xxxxx@yahoo.it – forzaitalia@comcast.net) risultavano riferibili ad utenti italiani.

Da una analisi sul web era possibile individuare sul sito xxx.it il riferimento della e-mail xxxxx@yahoo.it al nominativo di F.G. (indirizzo via ….. con telefono …..). Nominativo e riferimenti corrispondenti a quelli di F.G., dipendente del PAT.

Le ulteriori conferme ricavabili dall'analisi incrociata dei dati relativi alle connessioni al servizio VPN con account xxxxx@yahoo.it ed alle connessioni con Team Viewer come ricavati dal recupero dei dati presso il PAT consentono di affermare in questa fase (stante l'assoluta coincidenza dei collegamenti temporali riscontrati) che l'utilizzatore della casella di posta elettronica xxxxx@yahoo.it, collegatosi ai servzi di PROXPN attraverso l'**IP 85.88.202.118**, è il soggetto attaccante che ha effettuato l'accesso abusivo nel sistema informatico del PAT e lo ha quindi danneggiato mediante cancellazione dei dati ivi inseriti.

Risulta infine (a chiusura del cerchio) da ultime acquisizioni investigative che l'**IP 85.88.202.118** rientra in un *range* di otto indirizzi che **F.G. ha in affitto dal 2007 da Lineacom Srl**, società di servizi informatici del Comune di Pavia.

Detto compendio indiziario (già di per sé grave) acquista ulteriore forza e pregnanza se si considera che detto **F.G.** (attualmente impiegato in PAT presso la direzione Economica e Finanziaria) **dal 2004 al 2006 ha lavorato nell'Ufficio Sistemi Informativi dello stesso PAT, occupandosi per un certo periodo anche della gestione diretta della rete aziendale partecipando attivamente alla costruzione dell'architettura e delle infrastrutture**.

Dagli elementi raccolti nel corso delle indagini e sopra illustrati può certamente trarsi un grave quadro indiziario a carico di F.G. in ordine al delitto di cui agli artt. 81, 61 n° 11, 615 ter commi 1, 2 e 3 c.p. indicato nell'imputazione preliminare.

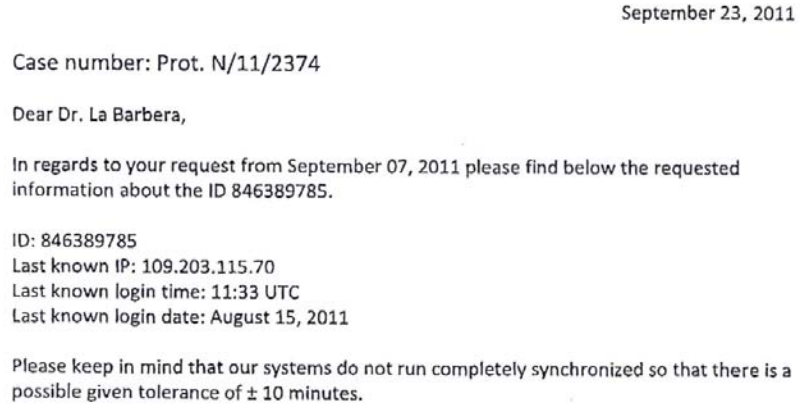
Successivamente si è celebrato, con rito ordinario, il relativo processo che ha portato alla condanna dell'imputato alla pena di anni 3 mesi 3 di reclusione[33].

Ci si trovava di fronte ad una aggressione informatica di particolare gravità che ha determinato **la perdita di una gran mole di dati, anche sanitari, relativi alle attività dell'ente pubblico Pio Albergo Trivulzio (PAT)** ed, in particolare, dei dati allocati sui 49 server virtuali e dei backup primari e secondari, pari a circa 3 Tera di dati: tali dati, seppur poi in gran parte successivamente recuperati, hanno in ogni caso cagionato un danneggiamento del sistema informatico del PAT con contestuale interruzione parziale del suo funzionamento e, con esso, di alcuni servizi resi all'utenza nei giorni successivi al Ferragosto 2011.

Vediamo nel prosieguo di mettere meglio a fuoco alcuni passaggi tecnico-investigativi fondamentali[34], secondo quanto è stato anche confermato dalla complessiva (e faticosa) istruttoria dibattimentale.

Come già ricordato, la polizia giudiziaria è stata in grado di restituire **l'analisi forense degli HD sequestrati il 18 agosto 2012, ed in particolare del computer in uso a G.M.** (dal quale si ritiene provata che sia avvenuta l'intrusione), analisi che confermava come

- **l'attacco sarebbe avvenuto dal PC del M. (PATHD02), utilizzando il programma Team Viewer, con l'ID 846389785** (come da risposta pervenuta dalla società produttrice, qui di seguito riportata):



September 23, 2011

Case number: Prot. N/11/2374

Dear Dr. La Barbera,

In regards to your request from September 07, 2011 please find below the requested information about the ID 846389785.

ID: 846389785
Last known IP: 109.203.115.70
Last known login time: 11:33 UTC
Last known login date: August 15, 2011

Please keep in mind that our systems do not run completely synchronized so that there is a possible given tolerance of ± 10 minutes.

- **l'intrusione è iniziata nel primo pomeriggio del 13 agosto (dalle ore 14.37[35] circa), protraendosi almeno sino alle 11.14[36] circa di Ferragosto;**
- **l'intruso possedeva la password di accesso mancando tracce su altre modalità di accesso al sistema:**

[33] Sentenza tribunale di Milano, n. 6993/20013 – est. Cotta. Confermata in Appello e passata in giudicato.

[34] Si farà da ora riferimento alla memoria di udienza del Pubblico Ministero Francesco Cajani depositata in sede di requisitoria e, per essa, ad alcuni passaggi delle relative trascrizioni di udienza.

[35] Orario UTC (GMT): sul punto vd. *infra* le considerazioni a commento esame consulente tecnico di parte.

[36] Orario UTC (GMT).

(teste GRANZIERA - ud. 8.7.2013, pp. 116 ss.)

P.M. – Va bene, quindi questo è il primo passaggio tecnico, poi... sto andando alle conclusioni, dite che appunto l'attacco è avvenuto dal computer di M., poi ***non ci sono tracce di attacchi al programma.***
TESTE GRANZIERA – No, assolutamente.
P.M. – E da qui fate dedurre una conclusione, che vorrei che però l'argomentasse meglio, cioè voi scrivete "Pertanto l'attaccante aveva a disposizione la password".
TESTE GRANZIERA – Certo.
P.M. – Spieghiamo meglio questo risultato?
TESTE GRANZIERA – Allora, TeamViewer è un notissimo programma per l'amministrazione remota dei sistemi, viene utilizzato sia a scopo commerciale che a scopo privato.
La rete TeamViewer è una rete un po' particolare, a dispetto delle altre tipologie di connessione remote, ad esempio VPN, la Software House che l'ha creato ha inventato, se possiamo dire, una metodologia di accesso con ID univoco, ed username univoco. Se come nel nostro caso il TeamViewer, quindi il programma ha due... parentesi, il programma ha due tipologie di installazione o l'installazione è istantanea, quella che scarica e fa partire direttamente il programma ed in quel momento viene assegnato un ID ed una password che è generata in maniera randomica; se invece come nel nostro caso è installato come servizio, perché appunto veniva utilizzato anche in altre maniere dal M., il programma rimane generalmente in memoria, il Pc rimane acceso con il programma che è attivo, per cui l'ID non cambia. Dal momento che è stata eseguita la prima installazione non esiste più, non viene più cambiato l'ID, si può cambiare la password, questo sì, però non esiste riuscire ad accedere alla macchina da remoto passando per questo sistema di autenticazione, anche perché l'autenticazione non è eseguita direttamente sulla macchina client, ma viene eseguita su un server che il più vicino è quello in Germania, poi ce ne sono altri sparsi in giro per il mondo. Avuta l'autenticazione al server il server fa la chiamata verso il client che risponde in modo tale da poter dare l'accesso al sistema client, ed in questo modo o si sa la password o si conosce la password o non si conosce, perché ***l'accesso avviene comunque in maniera diretta nel nostro caso, non è un tentativo di accesso tramite brute force, che sono attacchi particolari che vengono eseguiti, non vi è la presenza di questa tipologia di attacco, vi è proprio un accesso diretto alla macchina****.*

- **l'intruso ha cercato di nascondere le tracce dell'attacco cancellando il log di Team Viewer con la modalità "salva", cioè aprendo il file di log, cancellando quanto vi era memorizzato e poi salvando il file vuoto.**

Quest'ultima circostanza restituisce un importante dato comportamentale dell'autore del contestato reato: sicuramente esperto in informatica, sapeva che una mera cancellazione del file di log avrebbe creato sospetti negli investigatori (in quanto ogni programma informatico, di regola, tiene traccia delle proprie operazioni[37] e quindi una assenza di tal genere di file sarebbe fin da subito parsa inusuale) e portato ad un tentativo di recupero del file in ipotesi cancellato (sempre possibile laddove non si proceda alla sua distruzione con tecniche cd. di wiping)[38].

Da qui l'idea di far sparire le proprie tracce operando in una maniera differente[39], ossia cancellando il testo interno al file di log e procedendo poi al salvataggio del file (così diventato) vuoto (salvo il suo "messaggio di beffa", di cui si dirà). Ma tale tentativo, per quanto raffinato, non è stato in grado di vanificare la possibilità

[37] Ed in effetti, come noto, nella lingua inglese il termine log indica il diario di bordo di una nave, ma viene applicato estensivamente anche ad altri veicoli e macchine tra cui il computer. Nel gergo informatico, "loggare" (da verbo inglese to log) significa registrare all'esito di una attività di monitoraggio e quindi il log file (o file di log) è il risultato di tale operazione, che assume la forma di un file (di testo) nel quale vengono appunto indicate le operazioni che l'utente compie durante la sua sessione di lavoro.

L'opportunità di operare un tale monitoraggio può derivare da molteplici esigenze, tecniche (in caso di errore di un programma informatico, è necessario sapere le operazioni compiute dallo stesso nel momento immediatamente precedente), statistiche ed ovviamente di sicurezza (interna ed esterna).

[38] Trattasi infatti di procedura informatica particolarmente complessa e di non breve durata, idonea alla cancellazione in via permanente di un file.

[39] Cfr. teste CARBONE, ud. 8.7.2013, p. 45.

di recupero[40] di parte del testo originario, ritrovato dagli operanti di PG all'interno della parte non allocata dell'hard disk di M..

(teste GRANZIERA - ud. 8.7.2013, pp. 107 ss.)

TESTE GRANZIERA – Allora, la macchina di M., che possiamo chiamarla come testa di ponte dell'attacco verso la rete interna del PAT, del Trivulzio, parte appunto dall'accesso tramite TeamViewer. Sulla macchina di M., su un Pc che era in carico a M., che era stato successivamente, contestualmente al riconoscimento dell'attacco sequestrato e acquisito in un secondo momento e poi analizzato, sono state rinvenute numerose cancellazioni sia a livello di cartella di programma relativamente al TeamViewer, sia più che cancellazioni sovrascritture per l'esattezza, sia cancellazioni vere e proprie di dati presenti all'interno, presenti sul desktop ed in altre cartelle del personal computer.
Focalizziamo, ***viene focalizzata l'attenzione sul fatto che a seguito dell'intrusione tramite il software TeamViewer vi è la sovrascrittura****, quindi l'apertura del file di log dove il TeamViewer, dove il programma TeamViewer scrive tutte le connessioni in ingresso verso quella macchina, una sovrascrittura nel senso che c'è stata proprio una cancellazione di una parte di ogni stringa, ed* ***una sostituzione con la frase, con una frase in inglese se non ricordo male... scusi, un attimo, dovrebbe essere "Kiss my ass"****. La parte... questa sovrascrittura comporta anche a livello tecnico un'impossibilità a livello forense di andare a ripristinare quei settori sovrascritti in quanto vi è un'altra parola sopra e non è possibile andare a ricostruire un dato che è sovrascritto.*
P.M. – Questo file sovrascritto, mi scusi, qual era?
TESTE GRANZIERA – Il file relativo ai log TeamViewer.
P.M. – Ed è stato trovato nel luogo dove, di default TeamViewer lo colloca o no?
TESTE GRANZIERA – Sì, assolutamente sì.
P.M. – Prego.
TESTE GRANZIERA – Il Pc di M. oltre a questa sovrascrittura vi è anche tutta la parte di cancellazione ed il cambio di quello che è ***l'immagine del desktop*** *con un'altra immagine che rappresentava una figura, un artefatto di una figura a forma di scimmia con... in posizione un po' particolare. Detto ciò altre cose sono state..., all'interno del Pc di M. c'erano anche altre cose più particolari che ricordo, no, principalmente tutta la parte di TeamViewer, poi la cancellazione è stata eseguita su tutto quanto il Pc per cui quello che c'era prima è andato a cancellarsi a conclusione dell'attività.*
P.M. – Va bene. Allora voi vi aspettate di trovare i log di TeamViewer giusto, per andare a verificare qual è il codice abbinato a quel programma?
TESTE GRANZIERA – Sì, allora...
P.M. – E non lo trovate.
TESTE GRANZIERA – Eh...
P.M. – Perché ***al posto dei log ci sono queste scritte****.*
TESTE GRANZIERA – Sì, allora, il Pc di M. era un Pc chiave all'interno dell'infrastruttura del PAT, perché conteneva all'interno una serie di programmi per la connessione remota e per l'amministrazione anche remota, sia a livello tecnico che anche a livello meramente di accesso da parte di società esterne per esempio, che bypassavano il sistema di firewalling – parlo a livello tecnico, spero di essere abbastanza chiaro – che era praticamente a livello perimetrale, quindi esterno e che permetteva le connessioni verso l'interno della rete, del Pio Albergo Trivulzio, ma venivano direttamente inoltrate sulla sua macchina per convenienza probabilmente, e per facilità anche nell'utilizzo, e da lì si potevano muovere sui vari server virtuali in cui vi erano per esempio non so i programmi di amministrazione contabile piuttosto che lo storage dei dati generali. Da qui vi è..., ci sono appunto tutti questi... tra cui anche appunto il programma a cui abbiamo dato più importanza che era TeamViewer, perché gli abbiamo dato più importanza?
Perché ***ci siamo accorti che dall'analisi tecnica forense emergevano delle modifiche nelle date in cui è stato fatto, è stato eseguito l'attacco****. Noi ipotizzavamo al tempo una data che andava dal 13 al 15 di agosto, e giusto in quel periodo abbiamo visto il programma TeamViewer, abbiamo detto "Potrebbe essere effettivamente questo il programma con cui è stata fatta l'intrusione", andiamo a controllare e vediamo nei log appunto la modifica, la sovrascrittura. E soltanto successivamente dopo una* ***attenta verifica e ricostruzione di tutto quello che erano i settori attigui e contigui a quello che era il file modificato***

[40] **Ciò è stato possibile dal momento che il processo di creazione del log di Team Viewer lasciava, di volta in volta, tracce di sé all'interno dei file cd. temporanei del sistema informatico interessato: e dunque neppure la modifica del solo testo del log, operata dall'attaccante, ha impedito il recupero, seppur parziale, di tale informazione.**

abbiamo scoperto che vi era appunto un numero, un ID sessione, siamo riusciti a recuperare un ID sessione, che era il numero..., aspetti che glielo dico, che a memoria non me lo ricordo.
P.M. – Siamo a pagina 14.
TESTE GRANZIERA – Sì sì sì, un attimino solo. Sì, scusate. Sì, ***l'ID TeamViewer appunto 846389785****, che identificava in maniera inequivocabile l'accesso alla parte di un computer avente questo ID alla macchina di M., nella data, perché* ***l'ultima data che noi vediamo è quella del 15/08/2011 alle ore 11.14 circa in orario UTC****.*
P.M. – UTC significa?
TESTE GRANZIERA – Orario universale.
P.M. – Non ho sentito, scusi?
TESTE GRANZIERA – Universal Time Center, sì.
GIUDICE – È l'ora americana...
TESTE GRANZIERA – No, italiana.
P.M. – È italiana.
TESTE GRANZIERA – Europea.
P.M. – È Europea.
GIUDICE – Europea.
P.M. – Allora, poi torniamo a quella parte dove avete trovato questa informazione, però facciamo un passo in avanti, l'attacco voi dite "cioè vi è traccia dell'utilizzo di TeamViewer – e quindi dell'attacco – che finisce al 15 agosto 2011 alle ore 11.14", invece parte?
TESTE GRANZIERA – Parte il 13/08/2011 alle ore 14.37.
P.M. – Va bene. Allora, di regola l'ID, domando, dovrebbe essere contenuto nel file di log.
TESTE GRANZIERA – Sì.
P.M. – Okay, però scrivete che ***nel file di log non c'era, c'erano lo sovrascritture.***
TESTE GRANZIERA – Esatto.
P.M. – Quindi scendiamo a livello tecnico però è importante...
TESTE GRANZIERA – Certo.
P.M. – Questa informazione dov'è stata trovata e perché è stata trovata se qualcuno invece aveva tentato di cancellarla?
TESTE GRANZIERA – Allora, è stata trovata perché...
P.M. – Iniziamo, scusi, a dire dov'è stata trovata?
TESTE GRANZIERA – Allora, ***è stata trovata nei cluster non allocati, attigui a quello che era il settore dove era presente il file di log****.*
P.M. – Per i non tecnici ***cluster non allocati*** *significa?*
TESTE GRANZIERA – Sono i settori, basti pensare ad un foglio a quadretti, il file è compreso tra un quadretto numero 5 ed il quadretto numero 7, i quadretti precedenti e successivi fanno sempre parte di quel file e possono essere, si possono, possono essere presenti all'interno delle informazioni che in quel momento all'interno del file non ci sono più ma che lo erano perché non sono ancora stati sovrascritti, a differenza prima quando si cancella e si riscrive all'interno del file un determinato tipo di stringa in questo caso la cancellazione e basta comporta comunque il mantenimento all'interno di quelli parti che si chiamano appunto not allocate file, ovvero sia file non... parti, cluster non allocati, settori non allocati del disco.
P.M. – ***Quindi si cancellano, si pensano essere cancellati ma in realtà rimangono lì fin quando non si sovrascrive ulteriormente****.*
TESTE GRANZIERA – ***Certo, assolutamente.***
P.M. – ***Cosa che non è avvenuta in questo caso****.*
TESTE GRANZIERA – ***No, in questo caso non è avvenuta, infatti ci ha permesso di recuperare la stringa che ci interessava con l'ID di sessione****.*

(teste GARRISI - ud. 7.10.2013, pp. 79 ss.)

TESTE GARRISI – ***"kiss my ass" all'interno dei log.***
P.M. – Quindi era in questo caso, cioè era evidente che TeamViewer di regola non fa dei commenti...
TESTE GARRISI – ***Evidentemente manipolato, sì****.*
P.M. – Okay, però ugualmente l'allegate al cd?
TESTE GARRISI – Certo, sono allegate nel dvd dell'analisi.

P.M. – Quindi i log sono allegati al dvd, di cui chiederò la produzione. Come date conto della manipolazione dei file di log? Cioè al di là che si è trovata una frase che non è coerente con i log di TeamViewer, ci sono altre...
TESTE GARRISI – C'è una traccia all'interno del registro, ripeto, registro manipolato, quindi a poca valenza diciamo, però comunque c'è una traccia all'interno del registro del salvataggio del file "incoming.txt", in quanto evidentemente era stato..., evidentemente, è stato aperto con word e risalvato, praticamente salvando è rimasta traccia di questo salvataggio, non nella parte del disco ma nella parte del registro. Ripeto, sugli orari però e la data di questo salvataggio io non posso dir niente perché ripeto...
P.M. – Poi siamo a pagina 14, date atto, e qui... che ***comunque siete stati in grado di ritrovare log di TeamViewer che voi invece dite essere originali.***
TESTE GARRISI – Allora, noi abbiamo ritrovato nella parte non allocata del disco, la parte cancellata diciamo, quella non manipolabile se non con strumenti specifici, che abbiamo trovato dei log praticamente di questo TeamViewer, delle registrazioni di sessioni, noi le abbiamo prese e messe su dvd così come le abbiamo trovate, quasi tutte insomma, e dall'analisi fatta immediatamente abbiamo visto che l'attaccante praticamente aveva tra l'altro a disposizione un sistema operativo Ultimate Set, che è il Windows Seven praticamente, per cui non era un computer normalmente in utilizzo lì al Trivulzio.
P.M. – Ecco, ma sul giudizio di originalità rispetto invece ai log di TeamViewer, che li trovate dove ci si aspettava che cosa si può dire?
TESTE GARRISI – Allora, questi log sono dei log cancellati, totalmente cancellati, e generalmente anche TeamViewer cancella automaticamente insomma anche TeamViewer stesso i log. Quindi questi log qua potevano essere manipolati solo in modo, utilizzando un programma di file editing, anzi scusi, di file editing esadecimale, andava a toccare il disco fondamentalmente, quindi questi qua sono assolutamente...
P.M. – E quindi l'ipotesi che riportate per avvalorate la genuinità e quindi l'originalità, e non modificabilità... cioè non alterazioni di questi log qual è? Cioè che l'attaccante entra con TeamViewer e poi quali azioni fa per dissimulare le sue tracce ma in realtà poi rilascia...
TESTE GARRISI – C'erano dei log di TeamViewer lì chiaramente, perché TeamViewer salva questi log, quando è andato a modificare l'attaccante i file di log di TeamViewer, non so in che occasione o in che momento, chiaramente è andato a sovrascrivere quelli che già esistevano. ***Il problema è che anche a cancellare un file, anche a sovrascrivere un file il file se è lungo 100 caratteri ed io lo sovrascrivo con un file di 5 caratteri, sì è vero, quel file d'ora in poi sarà quello di 5 caratteri ma avrò 95 caratteri, per farla proprio semplice, che io potrò vedere nella parte non allocata del disco****.*
P.M. – Però è corretta, la stessa domanda in questi termini io alla fine ho cercata di farla anche al suo collega. È corretto dire, se così è l'ipotesi vostra, che l'attaccante cerca di cancellare il log, e quindi dalla parte vera ne sovrascrive una falsa, ma in quel momento però se ne rende conto meno, quella parte che cerca di cancellare comunque rimane sul computer.
TESTE GARRISI – ***Sì, in realtà l'attaccante era convinto probabilmente di averli cancellati.***
P.M. – Okay, ma il dato tecnico è che quella parte che si pensava venisse cancellata rimane insieme a quella nuova.
TESTE GARRISI – Rimane sì.
P.M. – ***E in questo date il carattere di originalità?***
TESTE GARRISI – ***Sì.***
P.M. – E da questa parte che trovate nel... prima di tutto vogliamo spiegare in termini sintetici e semplici che cosa significa parte non allocata del disco?
TESTE GARRISI – Come dicevo prima, quando... allora esiste il disco diviso in settori, cluster e così via insomma, esiste... quando io vado a cercare un file all'interno di un hard disk ci sarà un indice che dice "Guarda questo file inizia in questo settore e termina in questo settore". Quando il file viene cancellato non è che viene cancellato il file, viene cancellato quest'indice. La parte che rimane... io comunque questo file non è stato cancellato, fisicamente è ancora lì, salvo che non venga sovrascritto, questo è un altro discorso chiaramente. Se si agisce per tempo, diciamo, è ancora possibile recuperarlo quasi integralmente, tant'è che noi i file di log anche se non integralmente, ripeto, siamo riusciti ad acquisirli quasi integralmente, solo una piccola parte era stata sovrascritta.
P.M. – ***Okay. Quindi avete recuperato dei file di log che nell'ipotesi dovevano essere cancellati, e avete da lì estrapolato l'ID del programma TeamViewer****.*
TESTE GARRISI – ***Sì****.*

TESTE GARRISI – Pagina 14 io ce l'ho davanti. Allora, questa parte, che è la parte... mi dice che l'attacco è avvenuto utilizzando questo programma a partire dal 13 agosto 2011 alle 14.37, come ho detto prima, sino al 15 agosto 2011 alle 11.14 con questo ID.

*P.M. – **E scrivete "Allegato dvd", quindi significa che qua ci sono anche i file... all'interno del cestino che quelli nella parte non allocata.***

In tale iniziale contesto è stato pertanto possibile individuare una isolata[41] traccia, ossia il numero identificativo ID di una connessione effettuata da un computer remoto (esterno) mediante un particolare software (Team Viewer) risultata certamente riconducibile all'intrusione sotto i profili: **cronologico** (dentro l'intervallo del tempo di attacco, 13-15 agosto 2011), **funzionale** (realizzazione dell'accesso da una postazione esterna) e **strumentale** (tale ID è di per sé anonimo, e quindi utile allo scopo). In aggiunta, questo software (nella medesima versione free) veniva utilizzato – come è stato accertato – anche da altri utenti del servizio tecnico del PAT per accessi regolari dall'esterno e pertanto il suo utilizzo per fini illeciti, se accidentalmente scoperto da una analisi tecnica ordinaria, si sarebbe potuto spiegare quale accesso ordinario. E questa circostanza avrebbe potuto rappresentare altra forma di dissimulazione delle attività di intrusione. In realtà, le approfondite attività di analisi dei dati effettuate dal compartimento di polizia postale di Milano hanno fatto emergere la reale volontà dell'attaccante di inquinare le indagini nella sicurezza di rimanere ignoto, tanto da inserire nel file di log modificato persino la frase "kiss my ass" significativa della presunzione di non poter essere identificato.

(teste CARBONE - ud. 8.7.2013, p. 56)

TESTE CARBONE – La scimmietta sostanzialmente era un'immagine, un disegno animato, un semplice disegnino, non era nemmeno una scimmietta, era una sorta di pupazzetto colorato in atteggiamenti diciamo volgari a cui era aggregato un messaggio, questo messaggio si legge direttamente ed è riportato anche nelle analisi che poi sarebbero state svolte successivamente, o anzi eseguite e completate successivamente, e accompagna questo messaggio e si trova affianco al log della connessione, come una sorta di firma di chiusura.
P.M. – E questo messaggio che cosa riferisce?
TESTE CARBONE – Questo messaggio è in inglese e riferisce "Kiss my ass".
P.M. – Che significa? Tanto siamo persone tutte adulte.
TESTE CARBONE – Che volgarmente in inglese idiomaticamente vuol dire "Baciami il culo".

Quando si scarica il software Team Viewer l'utente lo riceve già contraddistinto da un ID univoco per ciascuno programma scaricato. Al lancio dell'applicazione per controllare, dal proprio computer, un computer fisicamente ubicato altrove, è necessario essere già collegati alla Rete internet. A seguito dell'avvio del citato software, la società tedesca proprietaria del programma riceve in automatico il numero IP[42] dell'utente che ne ha fatto uso con l'ID del programma scaricato. Sia il numero IP che l'identificativo ID sono dati che accompagnano le successive operazioni telematiche dell'utente.

Nel caso di specie, a seguito della modifica da parte dell'attaccante volta ad impedire la sua identificazione, il file di log degli accessi Team Viewer utile per le indagini non conteneva tale numero ID. Soltanto grazie alle operazioni tecniche di ricostruzione è stato possibile individuarlo, come già ricordato, in altra allocazione dei dischi.

Come già ricordato, è stato dunque il ritrovamento di questo ID durante la metodica analisi delle macchine distrutte dall'attaccante che ha permesso di ripercorrere, a ritroso, i passaggi prodromici all'attacco, tutti in origine assolutamente anonimi sotto il profilo telematico ma legati indissolubilmente tra loro.

Infatti, poiché l'analisi tecnica condotta aveva rivelato che l'attaccante si era dato da fare per cancellare oltre ai contenuti anche ogni traccia dell'attacco, sovrascrivendo anche i log del suo accesso in modo da renderli irriconoscibili, questo ID veniva fin da subito ritenuto dalla PG come quella unica "impronta" dalla quale poter partire.

[41] Trattandosi di versione gratuita di pubblico utilizzo (e non quella professionale, a pagamento) del programma Team Viewer, la società tedesca ha potuto segnalare l'accesso solo per l'ultimo utilizzo riferibile all'attaccante, così come avvenuto alle ore 11:30 circa del 15 agosto 2011. Per ogni utilizzo del programma Team Viewer acquistato con licenza d'uso, la società tedesca invece conserva tutto lo storico dei dati di connessione, ossia gli indirizzi IP degli utenti che l'hanno utilizzato.

[42] In questo caso, come anche accertato dall'istruttoria dibattimentale, il numero IP è in realtà quello assegnato dal servizio di anonimizzazione reso da PROXPN a cui si è collegato l'utente.

Nonostante l'ID Team Viewer "846389785" fosse collegato ad una versione free del software, scaricabile anonimamente dalla Rete (e con possibilità di tracciamento, come già ricordato, del solo ultimo collegamento registrato), la omonima società che commercializza il software Team Viewer collaborava pienamente alle richieste della autorità giudiziaria rilasciando esaurienti chiarimenti[43] a tutte le domande tecniche presentate dal personale della polizia postale di Milano: **si acquisiva così l'informazione secondo cui l'ID 846389785, rinvenuto a seguito di analisi tecnica quale traccia dell'attacco, alle ore 11:30 circa del 15.08.2011 era stato associato all'IP 109.203.115.70.**

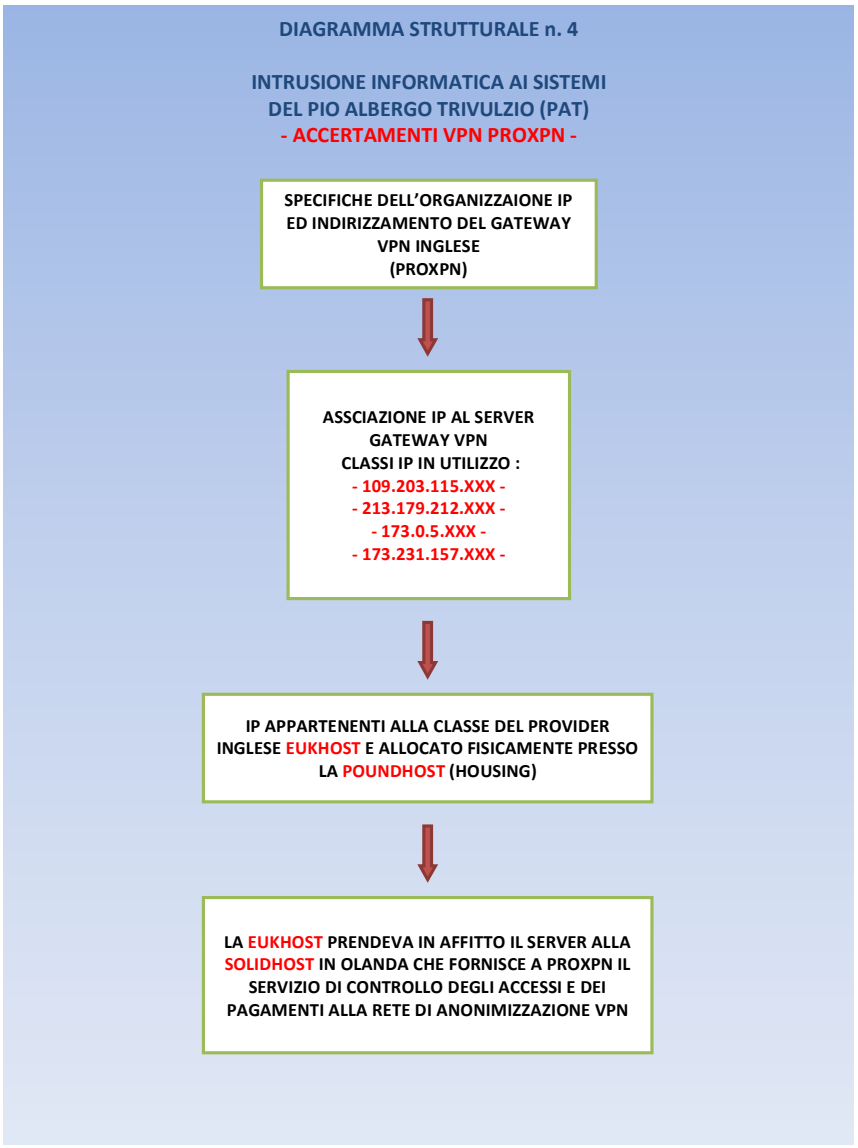
(teste CARBONE - ud. 8.7.2013, p. 56)

P.M. – Va bene. Quindi c'è questa interlocuzione con TeamViewer e quindi si fa un passo in avanti, giusto?
TESTE CARBONE – Sì fa un passo in avanti, sì. P.M. – Perché all'inizio abbiamo un identificativo di quella sezione e adesso invece in più abbiamo?
TESTE CARBONE – Abbiamo un indirizzo telematico […]

Iniziava così un lungo e faticoso tentativo di recuperare, tramite assistenza rogatoriale e grazie anche all'ottima cooperazione internazionale tra forze di polizia, le ulteriori informazioni utili ad identificare colui che si celasse sotto quell'IP identificato dalla polizia postale di Milano. E una corsa contro il tempo[44], atteso i termini di conservazione (pari a 12 mesi) dei dati attinenti al traffico telematico imposti dal nostro legislatore ai gestori di comunicazione.

[43] La risposta della società tedesca alla polizia postale è stata acquisita all'udienza del 19 dicembre 2013.

[44] Ed infatti gli ultimi decreti attinenti al traffico telematico sono stati richiesti, immediatamente dopo gli esiti ricevuti dall'Olanda, in data 7 agosto 2012, a quasi un anno dall'attacco informatico.



Dall'analisi ad opera della polizia britannica del server di PoundHost è emerso come al fine di collegarsi all'IP 109.203.115.70 l'utente avrebbe utilizzato il software della società PROXPN che utilizza le macchine di EUKHost.

PROXPN è una società che offre servizi per l'anonimizzazione dell'IP di collegamento, con connessioni VPN, ossia reti di telecomunicazione privata che sfruttano le linee pubbliche di trasmissione per ridurre i costi e fornire servizi aggiuntivi più efficaci e rapidi, soprattutto in Internet. Tanto per capire che cosa offra PROXPN vale la pena riprodurre l'*incipit* della home page[45] così come informalmente tradotto anche nella richiesta di misura cautelare:

> *"PROXPN è libera, facile da utilizzare, garantisce le tue connessioni Internet dalle intercettazioni, maschera la tua localizzazione e ti permette di accedere ai tuoi siti favoriti in assoluta libertà e da qualsiasi luogo – e poi prosegue ribadendo quali sono i suoi vantaggi – la Privacy online sta scomparendo. I governi censurano*

[45] Cfr. *http://proxpn.com/*

ogni informazione nel tentativo di lasciarvi all'oscuro. PROXPN ti permette di navigare liberamente in Rete senza pensieri e senza limiti"[46].

I motivi per i quali un utente della Rete si rivolge a PROXPN possono risultare innumerevoli ma appare altrettanto chiaro che tali servizi sono diretti a chi non gradisce essere facilmente rintracciabile. Infatti, il cliente finisce per apparire sulla Rete con un IP riferibile a Paesi diversi da quello dal quale opera: per la versione freeware appare in uscita da server statunitensi, mentre per quella con licenza d'uso può persino scegliere il Paese dal quale presentarsi.

Nonostante queste "precauzioni informatiche", le indagini – anche tramite assistenza rogatoriale[47] – sono state in grado di "svelare" tale tentativo di anonimizzazione, restituendo altre informazioni utili alla identificazione dell'attaccante.

[46] Il tutto con buona pace del consulente tecnico di parte, che durante il dibattimento aveva invece cercato di argomentare il contrario:

AVV. VERONELLI – Ecco, in relazione poi ad alcuni aspetti che sono emersi in questo processo io volevo che lei ci spiegasse esattamente ***la funzione del servizio di Proxpn****, come viene utilizzato dagli utenti e che tipo di servizio, se può essere considerato un sistema di anonimizzazione o che tipo di sistema di navigazioni è, e che finalità ha se è un utilizzo comune, presso quali utenti e per quali finalità?*

C.T. DIFESA – È un indirizzo comune per tutti gli utenti che hanno necessità per qualche motivo di utilizzare una linea di un altro stato. Ad esempio la Rai trasmette i contenuti video solamente agli utenti italiani e se un utente arriva su un sito della Rai con indirizzi IP non attribuiti ai numeri italiani non vede questi contenuti, allo stesso modo esiste chi, qualche Stato che trasmette partite di calcio solamente per i suoi cittadini o per i suoi blocchi di utenti. Nel caso specifico di ***F. mi spiegava che utilizzava le VPN per avere dei vantaggi nell'utilizzo di telefonate Voip****.*

È del tutto classico, si può immaginare che è come abitare alla frontiera con la Svizzera e andare al di là della dogana per comprare la benzina e fare benzina, in questo caso siccome internet permette la presenza in due parti del mondo qualunque esse siano quasi istantanea lui la utilizzava per effettuarci del traffico telefonico, comunque è normalmente utilizzato per questi motivi, i servizi di VPN commerciali. Questo è tutto.

AVV. VERONELLI – ***Questo, voglio dire, è un software di anonimizzazione classico o è semplicemente un software?***

C.T. DIFESA – ***Non lo chiamerei anonimizzazione.***

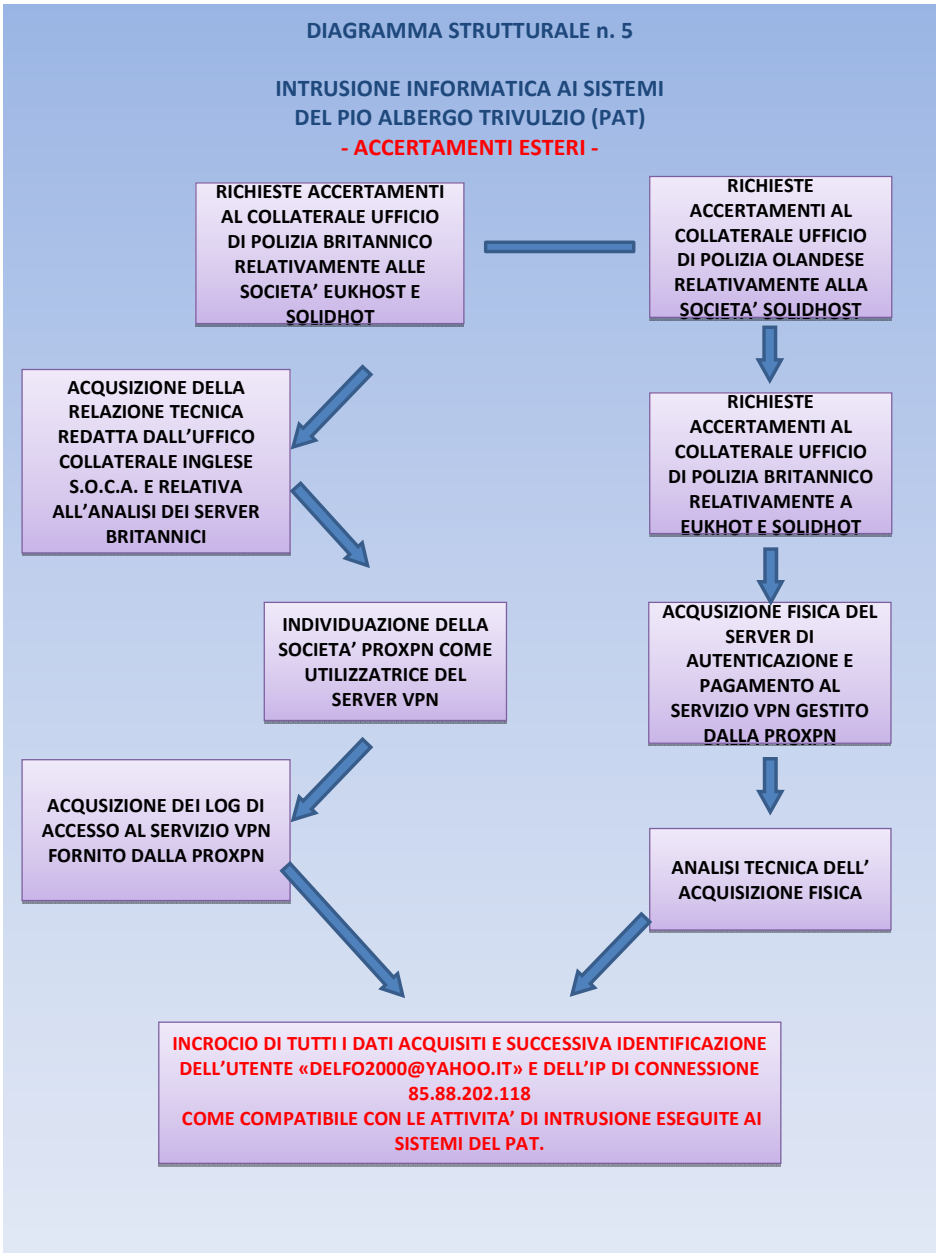
AVV. VERONELLI – Ecco, ci può dire com'è un software di anonimizzazione e cosa fa tecnicamente, abitualmente?

C.T. DIFESA – Un software di anonimizzazione, nella quale non specifico la mia attività di competenza nei primi due anni, quando funziona ed è disegnato correttamente, causa che nessun possa ricondurre un'attività ad un certo utente, un software di anonimizzazione forte fa questo, una VPN invece non è un software di anonimizzazione

perché è sempre un'entità come ad esempio Proxpn che può riconoscere l'utente cosa ha fatto, verso chi ha fatto del traffico, di conseguenza non lo chiamerei anonimizzazione, anonimizzazione in sé è questa sequenza dei servizi che riescono a rendere irrintracciabile il mittente con un altro tipo di connessione. Per questo motivo le VPN chiamo pseudo anonimizzazione perché c'è

sempre qualcuno che potrebbe ricondurre l'attività ad un certo utente. I servizi commerciali come Proxpn hanno la caratteristica di non dare l'anonimato e di comunicarlo già nella loro stessa dichiarazione perché se giustamente la Polizia deve fare delle indagini può riconoscere chi ha fatto le cose. In questo caso specifico mi sembra che Proxpn non abbia dato questo tipo di dato, cioè non abbia specificato cosa stesse facendo F. ma abbia solamente comunicato gli orario in cui lui si collegava.

[47] *Acquisite agli atti: sia in relazione alle risposte ottenute dall'Inghilterra sia quelle dall'Olanda.*



Peraltro, rileggendo i dati recuperati dal personal computer di M. e dalle macchine del PAT attaccate con i nuovi elementi raccolti in campo internazionale, **gli operatori di PG sono riusciti a scoprire ulteriori sessioni di accesso remoto effettuate dal numero ID Team Viewer "846389785" riconducendo a questo ID tutti gli attacchi effettuati sia tramite l'IP della classe 109.203.115.xx (sia tramite anche altri IP di PROXPN utilizzati per coprire la provenienza) nelle giornate dal 12 al 15 agosto 2011.**

A questo punto la polizia giudiziaria è stata in grado di incrociare tutti i dati a sua disposizione, nel modo descritto nella annotazione del 18 settembre 2011 (della quale sono state acquisite le tabelle che verranno di seguito riportate e commentate) e tenendo conto dello schema di attacco qui sotto nuovamente riprodotto:

A) In primo luogo si riporta nuovamente la tabella sintetica delle connessioni PROXPN realizzate dall'*account* dell'imputato durante quei giorni (così come indicata dalla polizia postale nella nota del 18 settembre 2012: gli orari, come indicato nella stessa nota, sono quelli americani EDT)[48]:

Orario connessioni al servizio *VPN*
(*account* delfo2000@yahoo.it)

	INIZIO connessione	FINE connessione	
delfo2000@yahoo.it	13 ago 2011 08:27	13 ago 2011 10:16	85.88.202.118
delfo2000@yahoo.it	13 ago 2011 13:09	13 ago 2011 15:37	85.88.202.118
delfo2000@yahoo.it	13 ago 2011 16:44	13 ago 2011 20:31	85.88.202.118
delfo2000@yahoo.it	13 ago 2011 21:02	13 ago 2011 21:04	85.88.202.118
delfo2000@yahoo.it	13 ago 2011 21:41	13 ago 2011 22:24	85.88.202.118
delfo2000@yahoo.it	14 ago 2011 05:08	14 ago 2011 05:11	85.88.202.118
delfo2000@yahoo.it	14 ago 2011 05:35	14 ago 2011 06:36	85.88.202.118
delfo2000@yahoo.it	14 ago 2011 08:05	14 ago 2011 09:43	85.88.202.118
delfo2000@yahoo.it	14 ago 2011 13:31	14 ago 2011 15:58	85.88.202.118
delfo2000@yahoo.it	15 ago 2011 05:32	15 ago 2011 05:43	85.88.202.118
delfo2000@yahoo.it	15 ago 2011 17:15	15 ago 2011 17:22	85.88.202.118

[48] pg. 1 e 2, acquisita all'udienza del 19.12.2013 e qui sotto riportata per comodità di lettura:

delfo2000@yahoo.it	8/13/2011 8:27[3]	8/13/2011 10:16	85.88.202.118
delfo2000@yahoo.it	8/13/2011 13:09	8/13/2011 15:37	85.88.202.118
delfo2000@yahoo.it	8/13/2011 16:44	8/13/2011 20:31	85.88.202.118
delfo2000@yahoo.it	8/13/2011 21:02	8/13/2011 21:04	85.88.202.118
delfo2000@yahoo.it	8/13/2011 21:41	8/13/2011 22:24	85.88.202.118
delfo2000@yahoo.it	8/14/2011 5:08	8/14/2011 5:11	85.88.202.118
delfo2000@yahoo.it	8/14/2011 5:35	8/14/2011 6:36	85.88.202.118
delfo2000@yahoo.it	8/14/2011 8:05	8/14/2011 9:43	85.88.202.118
delfo2000@yahoo.it	8/14/2011 13:31	8/14/2011 15:58	85.88.202.118
delfo2000@yahoo.it	8/15/2011 5:32	8/15/2011 5:43	85.88.202.118
delfo2000@yahoo.it	8/15/2011 17:15	8/15/2011 17:22	85.88.202.118

(teste GARRISI - ud. 7.10.2013, pp. 97 ss.)

P.M. – Mi scusi, seguiamo l'ordine dell'annotazione perché l'annotazione 18 settembre poi la produrrò con solamente le tabelle. Voi a pagina 1 mettete la prima tabella.
TESTE GARRISI – Noi mettiamo..., allora a ***pagina 1 ci sono le estrapolazioni praticamente di questa tabella che ci ha dato Kent Ball per tirare fuori quelli che erano i collegamenti con il 109 che arrivavano****...*
P.M. – Allora, qua... ripercorriamo le frasi così si capisce anche l'intento.
TESTE GARRISI – Sì.
P.M. – Voi all'inizio dite che avete contattato Kent Ball, giusto?
TESTE GARRISI – Sì.
P.M. – Poi dite che avete analizzato la classe di IP.
TESTE GARRISI – Abbiamo tirato fuori... allora, Kent Ball ci ha dato quest'elenco, abbiamo saputo contestualmente dagli inglesi che da quel server passava l'IP, la classe di IP 109, abbiamo cercato sui log che avevamo a disposizione, quelli cancellati, l'IP 109.
P.M. – Allora "Lo stesso", scrivete, "inviava una lista utenti che hanno utilizzato il servizio BPM(sic.) dalla macchina inglese sottoanalisi classe 109.203.115.xxx, che significa tutta la classe?
TESTE GARRISI – Xxx per me significa da 1 a 255.
P.M. – Riferito ad un periodo che va dal?
TESTE GARRISI – Dal 12 agosto 2011 al 15 agosto 2011, come ci ha riferito Kent Ball.
P.M. – E comunicando che l'orario...
TESTE GARRISI – Sì, Kent Ball nelle varie e-mail poi ci dice "Guarda che io non so sicuro dell'orario, se è meno quattro o meno cinque rispetto a GMT, ***e comunque è un Eastern U.S.A.", l'Eastern U.S.A. corrisponde a meno quattro, che più due sarebbe sei ore di differenza rispetto alle nostre****.*
P.M. – E quindi riproponete qui alla fine di pagina 1 la tabella che avevate utilizzato per richiedere i file di log.
TESTE GARRISI – Estrapolo da quella tabella che ci dà Kent Ball quelli riferiti a delfo2000. Questi sono i log riferiti a delfo2000.
P.M. – Va bene. Che sono gli stessi della tabella.
TESTE GARRISI – Sì, intanto...
P.M. – Okay, quindi con 8588202.
TESTE GARRISI – Esatto.
P.M. – Va bene.

B) Nella seguente tabella (riportata nel capo di imputazione così come indicata dalla polizia postale nella nota del 18 settembre 2011 senza gli evidenti errori di battitura quanto agli anni di riferimento, da intendersi ovviamente tutti riferiti al 2011)[49], si riportano invece le specifiche delle singole sessioni di Team Viewer, ritrovate nell'hard disk del Pio albergo Trivulzio in uso a M. a seguito della ricezione dell'elenco degli IP di PROXPN connessi con l'ID di Team Viewer (riferiti all'attacco):

[49] pg. 2, acquisita all'udienza del 19.12.2013 e qui sotto riportata per comodità di lettura:

16.37 13/08/2011	16.37 13/08/2011	213.179.212.76
16.45 13/08/2011	16.46 13/08/2011	213.179.212.76
16.47 13/08/2011	17.30 13/08/2011	213.179.212.76
19.09 13/08/2012	21.37 13/08/2012	109.203.115.89
22.45 13/08/2013	02.31 14/08/2013	109.203.115.71
02.39 14/08/2014	03.02 14/08/2014	213.179.212.122
03.05 14/08/2015	03.29 14/08/2015	173.231.157.74
03.42 14/08/2016	04.23 14/08/2016	109.203.115.66
19.33 14/08/2017	20.51 14/08/2017	109.203.115.109
21.11 14/08/2018	21.42 14/08/2018	109.203.115.109
22.10 14/08/2019	22.11 14/08/2019	213.179.212.70
23.47 14/08/2020	23.47 14/08/2011	213.179.212.69
01.38 15/08/2020	01.47 15/08/2020	173.0.5.51

Orario connessioni con Team Viewer
(recupero dati dell'analisi PC M.)

collegamento	inizio	fine	
13 ago 2011	16.37	16.37	**213.179.212.76**
13 ago 2011	16.45	16.46	**213.179.212.76**
13 ago 2011	16.47	17.30	**213.179.212.76**
13 ago 2011	19.09	21.37	**109.203.115.89**
13 ago 2011	22.45	02.31	**109.203.115.71**
14 ago 2011	02.39	03.02	**213.179.212.122**
14 ago 2011	03.05	03.29	**173.231.157.74**
14 ago 2011	03.42	04.23	**109.203.115.66**
14 ago 2011	19.33	20.51	**109.203.115.109**
14 ago 2011	21.11	21.42	**109.203.115.109**
14 ago 2011	22.10	22.11	**213.179.212.70**
14 ago 2011	23.47	23.47	**213.179.212.69**
15 ago 2011	01.38	01.47	**173.0.5.51**

(teste GARRISI - ud. 7.10.2013, pp. 98 ss.)

TESTE GARRISI – Intanto avevamo ottenuto da Linea Com Srl, che era l'assegnatario dell'IP 8588202118, avevamo ottenuto i log che ci dicono, praticamente che ci dicono, ci dichiara Linea Com essere assegnato direttamente come IP fisso a F.G., sin dal 2007, non ci sono riassegnazioni in corso. Quindi, allora a questo punto che cosa abbiamo fatto? ***A questo punto avendo un elenco di IP sicuri, da cui sono avvenute le connessioni con TeamViewer, siamo andati a rivedere di nuovo i file di log estrapolati****. Quindi, come dicevo prima, siamo riusciti a quel punto a capire come funzionavano i file di log di IP, a dare delle connessioni di inizio e di fine.* ***Tant'è che abbiamo trovato anche altri IP oltre ai 109, cioè i 213, i 173, che sono comunque IP di Proxpn.***
Abbiamo capito provando da noi praticamente come funzionava Proxpn, in pratica quando io pago per un servizio Proxpn, Proxpn mi collega una volta come voglio io o lo decido io o casualmente, mi collega con un server inglese o un server americano, e così via. In questo caso però noi non abbiamo potuto lavorare sul 213179 perché intanto oltretutto c'era stato un sequestro da parte della Polizia olandese dei server di Proxpn, per cui cosa abbiamo fatto? Abbiamo lavorato esclusivamente sull'IP che avevamo certi, cioè l'IP 109.
P.M. – Okay, però facciamo...
TESTE GARRISI – E li abbiamo confrontati con queste sessioni.
P.M. – Mi scusi, facciamo i passaggi delle tabelle, poi alcune vengono anche riprodotte poi nel capo d'imputazione.
Siamo a pagina 2, voi dite che allora c'è – l'abbiamo detto – i dati analizzati da Kent Ball, la conferma che l'8588202118 da richiesta all'Autorità Giudiziaria, che poi ha sentito anche il titolare di Linea Com, è sicuramente F., e ***poi c'è una tabella a metà di pagina 2.***
TESTE GARRISI – Sì.
P.M. – ***Che inizia con 16.37 del 13 agosto e finisce con 16.37 del 13 agosto.***
TESTE GARRISI – ***Come le dicevo, queste sono tutte le sessioni che noi siamo riusciti a ricostruire di TeamViewer****...*
P.M. – Le sessioni di TeamViewer ricostruite?
TESTE GARRISI – Sul pc di M., nella parte cancellata del disco.
P.M. – Questo significa che se noi per ipotesi dovessimo verificare, ma il Pubblico Ministero non ha nessun dubbio, questa tabella basta prendere il cd allegato all'annotazione e fare una ricerca per 213 e arriva questo log.
TESTE GARRISI – Sì.
P.M. – Quindi questa è la seconda tabella. Quindi da una parte...
TESTE GARRISI – Allora chiaramente...
P.M. – L'Olanda e dall'altra... praticamente questo è l'inizio dell'azione.

*TESTE GARRISI – Sì, **a questo punto noi avevamo dei log di TeamViewer, avevamo, e dei log che ci arrivano da Proxpn direttamente.** […] **abbiamo cercato di farli coincidere praticamente, come? Verificando gli orari e le date se coincidevano fondamentalmente, e abbiamo visto...***
*P.M. – Okay, e questa **è la tabella di pagina 2 finale?***
TESTE GARRISI – 2 finale, che i log di TeamViewer... i log, scusi, di TeamViewer erano all'interno o coincidevano quasi al secondo praticamente con i log che ci dava
Proxpn.
P.M. – Fine di pagina 2 è la tabella... seguiamo la tabella, fine di pagina 2 è?

*TESTE GARRISI – **A fine di pagina 2**[50] **abbiamo le connessioni quindi del 109, quelli di cui noi avevamo la certezza che ci dava Proxpn, cioè era una estrapolazione di questa tabella sopra solo con il 109**.*
P.M. – Quindi significa, leggiamo solo la prima riga e commentiamola?
TESTE GARRISI – Allora, "ore 19.09 13 agosto 2011 alle ore 21.37 del 13 agosto 2011 con IP 10920311589".
P.M. – Quindi chiedo la connessione a TeamViewer alle 19 e l'abbandono alle 21.37.
TESTE GARRISI – Alle 21.37 di TeamViewer.
P.M. – Va bene.
TESTE GARRISI – Abbiamo visto i file di log a questo punto di Proxpn e anche lì abbiamo...
P.M. – Scusate, scusate. Questa prima riga corrisponde alla quarta riga della tabella sopra.
*TESTE GARRISI – Sì, **corrisponde alla quarta riga.***
P.M. – Perché avete, di tutti i file di log avete estrapolato quelli 109203.
TESTE GARRISI – Perché noi abbiamo i log solo del 109, non avevamo i log del 213.
P.M. – Va bene. Quindi diciamo che, se ho capito bene, che la tabella di pagina 2 ultima è praticamente un sottoinsieme rispetto a quella...
TESTE GARRISI – Esatto, esatto.

Il confronto delle sole connessioni attuate con indirizzi di classe IP 109.203.115.xxx ricavate dal recupero dei dati appena menzionato nell'hard disk del Trivulzio in uso a M. con la lista di connessioni fornite da PROXPN relativamente all'account delfo2000@yahoo.it conduce alla seguente ultima tabella (così come indicata dalla polizia postale nella nota del 18 settembre 2011)[51]:

[50] pg. 2, acquisita all'udienza del 19.12.2013 e qui sotto riportata per comodità di lettura:

Di queste, le connessioni con classe di IP 109.203.115.xxx sono:

Inizio connessione con Team Viewer dalle	Fine connessione con Team Viewer alle	Ip utilizzato per la connessione
Ore 19.09 13/08/2011	Ore 21.37 13/08/2011	109.203.115.89
Ore 22.45 13/08/2011	Ore 02.31 14/08/2011	109.203.115.71
Ore 03.42 14/08/2011	Ore 04.23 14/08/2011	109.203.115.66
Ore 11.10 14/08/2011	Ore 11.10 14/08/2011	109.203.115.95
Ore 11.42 14/08/2011	Ore 12.16 14/08/2011	109.203.115.80
Ore 19.33 14/08/2011	Ore 21.42 14/08/2011	109.203.115.109

[51] pg. 3, acquisita all'udienza del 19.12.2013 e qui sotto riportata per comodità di lettura (**si noti che, a differenza di quanto effettuato dal consulente tecnico di parte, gli orari sia delle VPN che di Team Viewer sono stati tutti allineati tra loro** – cfr. nota 4 nella quale testualmente si precisa come "Gli orari delle connessioni in GMT-4 sono stati trasformati in GMT +2").

	Orario connessioni al servizio *VPN* (*account* delfo2000@yahoo.it)		**Orario connessioni con *Team Viewer*** (recupero dati dell'analisi al PAT)		
Data	**1 Inizio**	**4 Fine**	**2 Inizio**	**3 Fine**	**IP *(di copertura)***
13 ago 2011	**19:09**	**21:37**	**19.09**	**21.37**	109.203.115.89
13 ago 2011	**22:44**	**02:31**	**22.45**	**02.31**	109.203.115.71
14 ago 2011	**03:41**	**04:24**	**03.42**	**04.23**	109.203.115.66
14 ago 2011	**11:08**	**11:11**	**11.10**	**11.10**	109.203.115.95
14 ago 2011	**11:35**	**12:36**	**11.42**	**12.16**	109.203.115.80
14 ago 2011	**19:31**	**21:58**	**19.33**	**21.42**	109.203.115.109

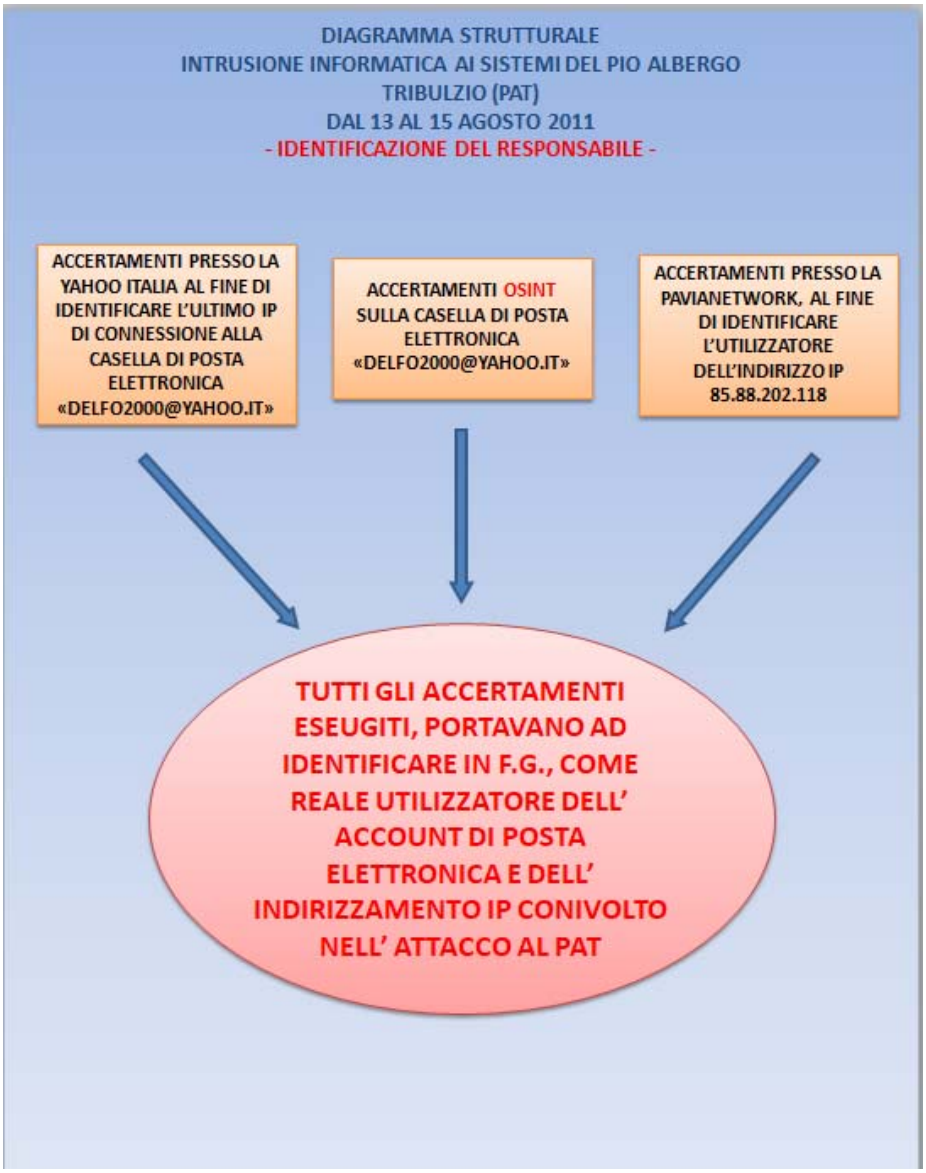
Ebbene, **questa assoluta coincidenza dei collegamenti temporali riscontrati in due situazioni diverse, gli uni provenienti dalle registrazioni dei log olandesi di PROXPN, gli altri dai dati presenti nell'hard disk del PAT recuperato ed in uso al M., riaggregati ed analizzati, dimostra in maniera inequivocabile che l'utilizzatore della casella di posta elettronica delfo2000@yahoo.it (imputato), collegatosi ai servizi di PROXPN attraverso l'IP 85.88.202.118, è certamente l'attaccante che – previo accesso abusivo – ha danneggiato il sistema informatico del Pio albergo Trivulzio operando durante i giorni 13, 14 e 15 agosto 2011 e, all'esito, ha eliminato le tracce del programma da lui utilizzato sostituendovi la frase "kiss my ass".**

Ma ci sono anche altri riscontri positivi che confermano l'ipotesi accusatoria, come indicati nel diagramma seguente:

Tutta questa attività di analisi ha permesso di effettuare un confronto tra dati di fonti diverse: l'estrazione delle singole connessioni degli attacchi (dal computer di l)) e i dati forniti da l l (relativi alla classe 109).

Il risultato è la tabella di seguito[4]:

mail	Inizio connessione al servizio VPN	Fine connessione al servizio VPN	Inizio connessione/i con Team Viewer	Fine connessione/i con Team Viewer	Ip utilizzato per la connessione/i
delfo2000@yahoo.it	8/13/2011 19:09	8/13/2011 21:37	19.09 13/08/2011	21.37 13/08/2011	109.203.115.89
delfo2000@yahoo.it	8/13/2011 22:44	8/14/2011 02:31	22.45 13/08/2011	02.31 14/08/2011	109.203.115.71
delfo2000@yahoo.it	8/14/2011 03:41	8/14/2011 04:24	03.42 14/08/2011	04.23 14/08/2011	109.203.115.66
delfo2000@yahoo.it	8/14/2011 11:08	8/14/2011 11:11	11.10 14/08/2011	11.10 14/08/2011	109.203.115.95
delfo2000@yahoo.it	8/14/2011 11:35	8/14/2011 12:36	11.42 14/08/2011	12.16 14/08/2011	109.203.115.80
delfo2000@yahoo.it	8/14/2011 19:31	8/14/2011 21:58	19.33 14/08/2011	21.42 14/08/2011	109.203.115.109



In particolare, **l'IP 85.88.202.118[52] rientra in un range di otto indirizzi che l'imputato aveva in affitto, fin dal 2007, da Lineacom Srl, società di servizi informatici del Comune di Pavia.**

L'imputato, per tutto il corso del processo[53], ha sempre affermato la sua estraneità ai fatti:

> *IMP. – Perfetto. Io a questo punto le faccio notare,visto che abbiamo fatto richiesta, e voi ci avete accordato senza nessun problema, del supporto informatico, abbiamo controllato ed è pieno zeppo di incongruenze per quanto ci riguarda, per quanto mi riguarda.*
> *P.M. – Scusi,* ***"abbiamo controllato" intende dire lei e il suo Avvocato o lei e il suo consulente? Chi?***
> *IMP. – Io e il consulente, il nostro consulente.*
> *P.M. – Lei e il consulente che dovremo sentire, giusto?*
> *IMP. – Sì sì, non c'è nessun problema.*
> *P.M. – … cerchiamo di capire il cuore del problema.* ***C'è un'evidenza di uso di Team Viewer in uno qualsiasi dei computer trovati a casa sua, sì o no?***

[52] Cfr. teste GRANZIERA (ud. 7.8.2013, p. 131).

[53] Anche nel processo di fronte alla Corte di Appello, l'imputato ha mantenuto la stessa linea difensiva. Pur tuttavia, pur essendo stata richiesta e ammessa una consulenza tecnica di ufficio (ad opera dell'ing. Francesco Picasso), essa ha ancora una volta confermato i risultati investigativi emersi in primo grado dalle indagini della Polizia Postale di Milano.

*IMP. – **No no.***
P.M. – Come no? Lo dice lei che il suo consulente ci verrà a dire che c'è un Team Viewer sul computer secondo lei sbagliato.
IMP. – No no, lei sta dicendo l'uso. Quello che voi trovate sono delle definizioni che sono scaricabili da Internet, che lo fa Snort e ne abbiamo già parlato.

P.M. – […] Torniamo sempre su quanto ritrovato sui computer e sempre all'annotazione che stiamo commentando insieme, perché anche qui questa è una tabella che è stata acquisita all'esito poi dell'esame della Polizia Postale. Siamo a pagina 14. La Polizia Postale dà atto che, e l'ha riferito in udienza, per la parte valutativa ci sarebbero evidenze di ultimi file aperti su uno dei suoi computer il giorno prima della perquisizione, e quindi il giorno nel quale si è verificato l'episodio che sua sorella oggi ha raccontato, in relazione per esempio alla cartella su un'applicazione denominata "T110/wd_tb1", per esempio "analisi – lo si deduce dal nome – lavoro Giovanni server Trivulzio".
*Altrimenti sempre cartella "important/documenti lavoro". Anche qui sempre da questo supporto "mansioni dipendenti B.L.S.". **Quindi dice la Polizia in udienza che abbiamo ricerche il giorno prim dell'arresto su un supporto che non è stato ritrovato. Allora, dividiamo la domanda in due parti: sono effettivamente ricerche che lei ha fatto il giorno prima dell'arresto e se sì per quale motivo?***
*IMP. – **Che io mi ricordi no**.*
*P.M. – **Lei insieme al suo consulente, visto che ha fatto la verifica, ha ritrovato questa evidenza informatica sui computer o no? O la contesta anche in questo caso?***
*IMP. – **Per l'esattezza noi questo computer, visto che non aveva nulla per il momento che ci interessava, non l'abbiamo ancora guardato. Pertanto su questo non le posso dare un'indicazione**.*

P.M. – Va bene, prendiamo atto della sua risposta, signor F. Questo hard disk lo vuole fornire alla Polizia Giudiziaria, o no?
IMP. – Ma quale hard disk?
P.M. – Quello denominato "T110/wd_tb1".
IMP. – Ma non c'era un hard disk, erano lì per terra. Quelli che c'erano erano per terra, li abbiamo indicati.
P.M. – Sì, ma le cartelle stanno su un hard disk e non stanno sulla memoria.
IMP. – Stanno su un supporto.
P.M. – Sì, il supporto si chiama hard disk dove ci sono le cartelle, perché anche le memorie flash non hanno delle sotto directory. Per cui se vogliamo fare un contraddittorio tecnico ha filo da torcere con questo Pubblico Ministero, va bene?
IMP. – No no no.
*P.M. – Però **risponda alle domande non in senso tecnico. Le chiedo: c'è un hard disk mancante, sì o no?***
*IMP. – **Le rispondo quando mi sono consultato col mio consulente.***
P.M. – Va bene, prendo atto che a questa domanda non vuole rispondere ed è un suo diritto. Andiamo avanti.

*P.M. – […] pagina 14: si trova, e questo dovrebbe essere di fondamentale importanza, **un file denominato "Pas.txt"** che contiene delle password e avrà sentito con le sue orecchie Durante[54]. Alla prima udienza dice che la password "gioveadministrator" è una password: 1), che era a conoscenza solo del ristretto gruppo tecnico del PAT; 2), era la password di super amministratore, cioè testuali parole di Durante "consentiva l'accesso a tutte le macchine del PAT". Domanda: come si spiega questa password sia stata ritrovata sul suo computer?*
IMP. – Allora, queste password io le ho avute quando sono ritornato in servizio. Io sono ritornato in servizio un anno dopo l'attacco, più di un anno dopo l'attacco. Quello che lei mi sta dicendo...
P.M. – Scusi, come può logicamente giustificare questa affermazione visto che lei, l'abbiamo analizzato sotto vari profili, lei era stato allontanato da funzioni tecniche anni prima dell'assalto? Quindi come è possibile sconfessare, perché lei sta sconfessando un Teste, dicendo che era... qualcuno gliele aveva date legittimamente?
*IMP. – Se mi lascia parlare. Io sono ritornato in servizio, io **sono ritornato ai sistemi informativi un anno dopo, nel luglio del 2012. Io le ho ricevute lì queste password.***
P.M. – Nel?
IMP. – Luglio del 2012.

[54] Trattasi del responsabile servizi informatici del Pio Albergo Trivulzio.

P.M. – E per quale motivo le ha ricevute?
IMP. – Per lavorare. Io attualmente – va bene, sono sospeso – risulto in servizio presso i sistemi informativi se no io come faccio a fare qualsiasi lavoro, qualsiasi...?
P.M. – Va bene, ***non ricordo*** *(e l'avrà verificato anche lei)* ***che Durante abbia fatto il suo cognome tra le sue persone legittimate ad avere questa password****, perché ha detto B, ha detto G., ha detto M., non ha detto F..*
IMP. – ***Qui stiamo parlando di due anni diversi, io non so quelle password che c'erano prima***[55]***.***
P.M. – No, Durante, se vuole le prendo il passo...
IMP. – No no, ma io ho presente quello che...
P.M. – Siamo a pagina 18 dell'udienza dell'8 luglio 2013.
IMP. – Ho capito, io non so quali fossero le password del 2011, se è quello che intende dire lei.
P.M. – No, non è quello che intendo dire io. Io intendo dire che lei quelle password nel 2011 e nel 201 non le doveva avere.
IMP.– Ma nel 2012.
P.M. – Questo è quello che dice Durante. Nel 2011 e nel 2012, cioè 2011 all'epoca dell'attacco e nel 2012 all'epoca della perquisizione non le doveva avere. E questo non lo dico io, lo dice Durante.
IMP. – ***Posso fare però una precisazione? Queste password al fine della ricostruzione dell'attacco della Polizia Postale sono assolutamente inutili, non sono servite a nulla in qualsiasi lei la veda****.*
P.M. – Allora, pagina 18, Pubblico Ministero: "La conoscenza di queste password cosa comportava?" "Consentiva l'accesso a qualsiasi sistema all'interno della rete aziendale".
IMP. – Sì, però nella ricostruzione...
P.M. – E poi prima ancora dice che riconosce come password attiva e funzionante la prima "gioveadministrator??v14marostica".
IMP. – Va bene.
P.M. – Quindi questo le voglio dire, che Durante dice che erano password di super user attive e che erano nella disponibilità e nella conoscenza legittima solamente di persone, tra cui F. non c'era.
IMP. – Non c'era nel 2011. Io nel 2012 sono tornato
ai sistemi informativi.
P.M. – ***Da chi le avrebbe ricevute?***
IMP. – ***Non me lo ricordo, erano in rete****, le ho copiate quando mi è stato detto che dovevo fare dei lavori. Poi ho avuto i problemi di salute...*
P.M. – Con queste password cosa doveva fare?
IMP. – Se io sono ai sistemi informativi dovevo fare degli interventi.
P.M. – Mi dica quali interventi doveva fare con queste password.
IMP. – Non li ho fatti perché sono andato in malattia per i problemi di salute, ma se uno deve farli come fa a fare interventi di vario genere sul computer se non ha accesso?
P.M. – Va bene, le ha mai utilizzate queste password, o no'
IMP. – Mai, all'atto pratico mai.
[…]P.M. – … può anche non rispondere alla domanda, però la deve dire, non deve girare intorno ogni volta. Le chiedo: come mai queste password che lei aveva, che lei legittimamente aveva, e teniamo buona la sua versione, le abbiamo trovate nel computer di casa e non in ufficio?
Questa è la domanda.
IMP. – Ma perché queste qui ***io me le sono segnate su un pezzo di carta che avevo nel portafoglio****.* ***Quando sono arrivato a casa che ero in malattia le ho semplicemente registrate lì sul mio computer, punto e basta, per tenerne memoria, ma io ero a casa.***
P.M. – Va bene, ce le ha sotto mano? È la password giove è quella di super amministratore?
IMP. – Sembra di sì, c'è scritto "administrator".
P.M. – Non lo so, me lo deve dire lei perché le aveva richieste per utilizzarle.
IMP. – Allora, lei non ha ancora capito che io quando sono tornato ai sistemi informativi poi ho avuto un problema di salute e mi sono riassentato, pertanto non ho di fatto preso neanche atto di come funzionava, niente.
P.M. – Va bene. "Acronix" invece?
IMP. – Molto probabilmente è un utente di backup.
P.M. – "Temadmin?"(?)
IMP. – Lo ignoro, saranno utenti che serviranno a qualcosa su sistemi, come GPI(?).

[55] Si noti invece come DURANTE avesse riferito che la password di super.user, ritrovata sul pc dell'imputato, fosse **quella attiva e funzionante al momento dell'attacco.**

P.M. – ***Quindi lei ha delle password che dice non aver mai utilizzato, ma non sapeva neanche a cosa servissero?***
Neanche il giorno che le ha richieste, che le ha segnate sul foglio di carta si è fatto la domanda "ma queste password a cosa mi servono?"

IMP. – ***Nel senso che la relazione a firma mi pare Granziera, che ho qui, per esempio non c'è neanche l'IP mio, c'è solo il mio indirizzo di posta elettronica, la password.*** *Io non sono neanche in grado di dire se questo l'ha generato realmente il mio computer o il sistema di proXPN che per gli affari suoi si sta facendo dei calcoli. Non c'è neanche l'IP e l'avete messo voi questo.*
P.M. – ***No, c'è.***
IMP. – ***No no.***
P.M. – C'è sul server...
IMP. – Olandese.
P.M. – Su quell'hard disk che è copia del server olandese c'è a ritroso l'IP che proXPN le dà per navigare anonimo, ma prima di questo regalo – che poi non è regalo perché lei ha pagato il servizio – c'è il suo IP abbinato alla sua casella perché proXPN non è nient'altro che un sistema di anonimizzazione, io gli chiedo un IP per navigare indistintamente, lui tiene traccia del mio IP e mi dà un IP diverso. Io con quell'IP diverso navigo, tant'è vero che sul computer target (inc.) non abbiamo trovato il suo IP, abbiamo trovato l'IP di proXPN. Quindi c'è tutto qui.
IMP. – ***Forse stiamo parlando di due relazioni diverse e dei file di log.***
P.M. – Mi dica.
IMP. – No, me lo dica lei. Io ho in mano quella del 28 gennaio.
P.M. – 28 gennaio, mi dica la tabella.
IMP. – No, 28 gennaio, è a firma...
P.M. – Sì, mi dica la tabella di pagina visto che le abbiamo tutte... forse non ci sono le pagine, però contiamo. Qual è la tabella?
IMP. – ***Io non vedo il mio IP. Lei dove lo vede il mio IP su queste che lei definisce connessioni? Dov'è? Me lo faccia vedere, io non lo vedo, scusi.*** *Stiamo parlando della stessa relazione, dov'è l'IP mio? Io non sono neanche in grado di dirle se queste sono connessioni che ho fatto io.*
P.M. – Sono connessioni richieste da delfo2000@yahoo.it, casella di cui lei anche di fronte al G.I.P. ha ammesso l'utilizzo esclusivo.
IMP. – Ma io le ho appena detto...
P.M. – Conferma questa cosa, che lei come aveva già detto è l'unico esclusivo utilizzatore di delfo2000@yahoo.it?
IMP. – Le sto spiegando...
P.M. – No, mi deve rispondere a questa domanda che è semplicissima.
IMP. – Sì sì.
P.M. – Vuole fare un passo indietro rispetto alle dichiarazioni del G.I.P. e ne prendiamo atto, conferma?
IMP. – No no, ma delfo2000 la uso io dal 1999 senza nessun problema. Però, come le ho già detto, su queste tabelle qui non c'è il mio IP, è questo che non riesco a capire.
P.M. – Va bene, prendiamo atto anche di queste sue risposte.
Poi a dire il vero, ma giusto perché mi vuole portare sul piano tecnico, a pagina 3 c'è una richiesta di autenticazione con l'IP, richiesta dell'autenticazione 8588202114.
IMP. – E infatti non è l'IP dell'attacco che voi mi attribuite.
P.M. – È uno dei suoi IP?
IMP. – Sì, ma non è quello dell'attacco. Bella questa cosa, giusto per dirlo.
P.M. – Infatti è del 6 agosto 2011.
IMP. – Ma, attenzione, non è dell'attacco.
P.M. – Quindi questa che lei dice è un'attività che lei ha fatto, si ricorda di aver fatto questa attività?
IMP. – Molto probabilmente sì, questa è...
P.M. – È relativa a un pagamento.
IMP. – Può essere, ci mancherebbe.
P.M. – Perché sui pagamenti, l'avevamo già chiarito, eventualmente se lo vuole richiarire, lei ammette di aver fatto dei pagamenti ad agosto. ***In particolare c'è la traccia del 6 agosto, il rinnovo, ma di aver fatto dei pagamenti anche in precedenza, giusto?***
IMP. – ***Sì, penso di sì.***

IMP. – No, ***molto probabilmente mi trovavo a casa,***

date anche le condizioni di salute di mia mamma ragionevolmente mi trovavo a casa. Non ho problemi di ammettere questo.
P.M. – Quindi lei non si ricorda comunque se in quei giorni ha usato proXPN.
IMP. – No. Però lei deve tener conto...
*P.M. – **Però lei ha usato proXPN indipendentemente da quei giorni o no?***
*IMP. – **Sì sì.***
P.M. – Allora, vogliamo chiarire quell'affermazione che ha fatto al G.I.P.? Perché poi da quell'affermazione è emersa un'intercettazione che lei avrà visto perché è stata già depositata.
IMP. – Sì sì.
P.M. – L'intercettazione tra tale M. e il padre in cui parlando di lei si dice che F. utilizzava proXPN perché, appunto, gli consentiva...
IMP. – No no, non dicono che utilizzavo proXPN, dicono la VPN.
P.M. – Prima di tutto spieghi chi è questo M., lei lo conosce?
IMP. – È un amico.
P.M. – Un caro amico?
IMP. – Un amico, sì.
P.M. – È un suo caro amico?
IMP. – Sì.
*P.M. – **E il senso di quella intercettazione il cui testo a questo punto lo diamo per letto[56] qual è?***
*IMP. – **Lo doveva chiedere a lui, sta parlando con suo padre, non è che sta parlando con me. Sa, uno quando parla con qualcuno può dire quello che vuole.***
P.M. – Certo, però immagino che M. non è che sappia di lei cose che non ha mai sentito dire da lei.
IMP. – No, però non è neanche uno che si occupa più di tanto di informatica. Ogni tanto mi chiede qualcosa, glielo faccio vedere e può ben essere che capisce e non capisce, come una cosa normale, come il sottoscritto parla con gli Avvocati e capisce e non capisce di processi penali. È una cosa normale.
*P.M. – **Il M. dice il vero delle sue attività, o no?***
IMP. – No, dice il vero, ma io partecipo anche come volontario a un progetto universitario delle VPN, se è per quello, che io suoi uomini stranamente non hanno visto sui miei computer.
*P.M. – Quindi **lei vuole sostenere che il M. dice il vero sul fatto che lei sapeva che era anonimo, però per fini leciti?***
*IMP. – **No, M. stava parlando di VPN, a dire la verità lui parlava di tunnel VPN e io le ho appena detto che di VPN – a parte proXPN che è alla luce del giorno, una cosa normalissima – alla luce del giorno c'è un progetto universitario che io seguo**, che c'è anche il programmino installato sulla mia macchina virtuale che mi avete sequestrato e stranamente non avete notato che quella è una VPN che è un progetto universitario. Non l'avete notata, non l'avete sottolineata, che è una cosa un po' strana.*

---

[56] Cfr. trascrizione telefonata n. 68 del giorno 16/11/2012, ore 15.02.21:

*PAOLO: **E perché da quello che raccontava questo**... ma questo **due o tre anni prima che succedessero i vari casini**, ti ricordi?*

SIMO: (Inc.)

PAOLO: Tre/quattro anni fa.

SIMO: Però certo ...

PAOLO: Però combinare una roba così è grossa! Ma non so io!

*SIMO: Ma **io so che lui utilizzava dei tunnel, un tunnel dentro l'altro tunnel, usava ste cagate così, però poi. io infatti glielo dicevo "ma secondo te comunque è riconducibile se tu fai un reato, una roba del genere, qua comunque ... arrivano a te"** ...*

PAOLO: Eh sì, una traccia c'è.

SIMO: " ... una volta che trovano (inc. I sovrapporsi di voci) .. "

PAOLO: Una traccia c'è ...

*SIMO: "**Sì, ma no, diventa difficile, perché poi passi attraverso gli altri paesi ...** ", col cazzo! Qua tre paesi ... tre paesi han fatto ... han fatto le indagini.*

PAOLO: Ma che pistola! Va beh dai, Simo, adesso vado. Ci sentiamo.

Il processo infine ha registrato un clamoroso colpo di scena, all'udienza del 7 aprile 2014, a seguito del maldestro tentativo del consulente di parte di sconfessare i risultati delle analisi compiute dalla polizia postale di Milano:

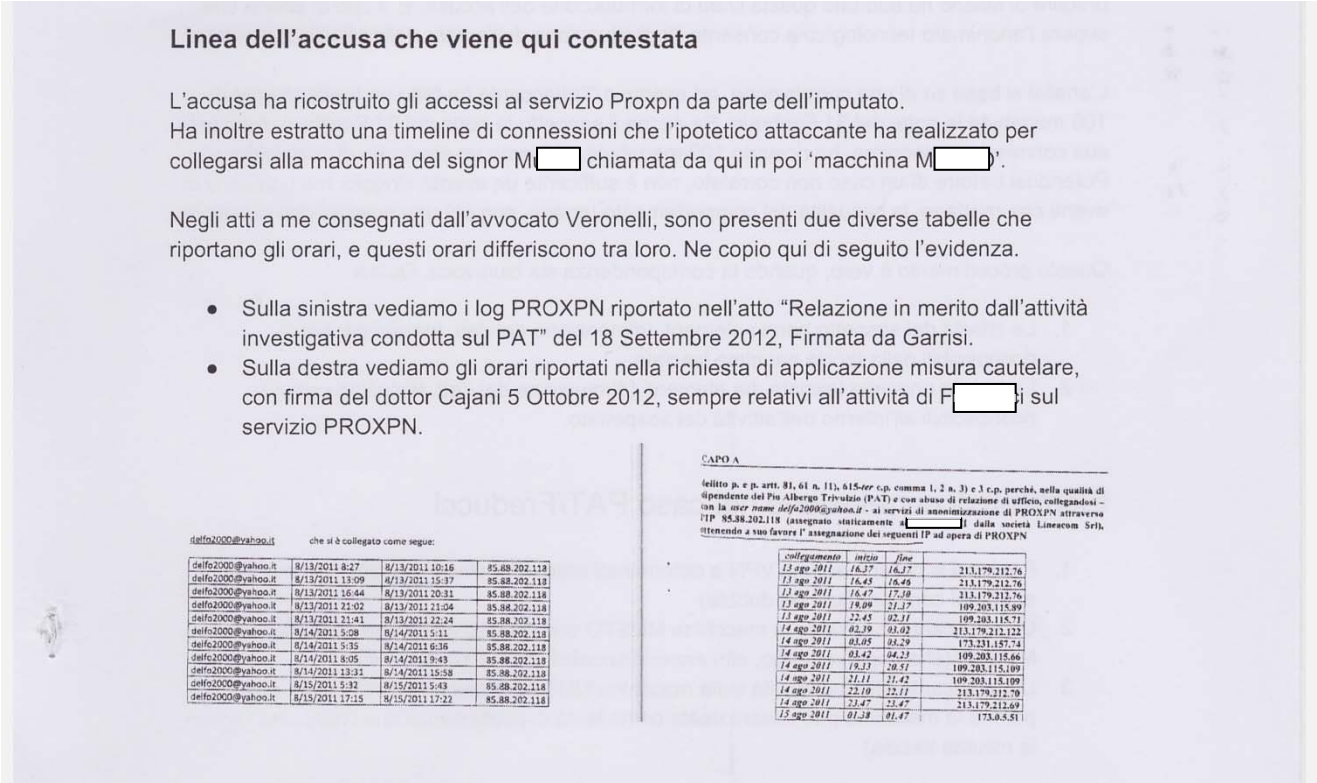
> *P.M. – Ma lei prima di questo processo ha avuto* ***esperienze di consulenza*** *di fronte all'Autorità Giudiziaria?*
> *C.T. DIFESA – no, ho una grande (inc.) tecnologica, di conseguenza ho fatto insegnamento in questi ambiti ma mai esperienza pratica.*
>
> *C.T. DIFESA – Ho ricevuto su una chiavetta USB dall'Avvocato Veronelli tutti gli atti in formato PDF, ho ricevuto gli stessi atti anche in copia cartacea, poi un* ***hard disk contenente PATHD01[57], PATHD02*** *e l'hard disk acquisito a casa del F., e poi l'integrazione nell'ultimo mese di un disco a 3 Giga contenente i tre Raid, i* ***tre dischi Raid della macchina NAS[58]****, e anche altri due hard disk che non erano parte del mio questionario, non ho controllato. Questi quindi.*
> *P.M. – Va bene, continuiamo sulle sue considerazioni, "****La stringa trovata non è un log, è un file di configurazione di un altro software, Snort****".*
> *C.T. DIFESA – Sì.*
> *P.M. –* ***Questo programma cosa fa?***
> *C.T. DIFESA –* ***questo programma serve per individuare intrusioni nelle reti, quindi individuare dell'attività di rete non prevista.***
> *P.M. – è normale trovare un programma del genere su un computer di una persona di normale esperienza tecnologica o no?*
> *C.T. DIFESA – Di una persona di normale esperienza no,* ***non so se F. lei lo considerava di normale esperienza visto che è un programmatore ed un sistemista.***
> *P.M. –* ***lei sa che F. è un programmatore e sistemista da quali****...*
> *C.T. DIFESA –* ***perché me l'ha detto lui****, cioè quindi ammetto che era una mia considerazione personale il fatto che è plausibile che lui utilizzi questi sistemi, comunque sia ha avuto competenza anche di spiegarmi perché lo utilizzava, mi ha mostrato la macchina virtuale, che in una macchina virtuale... anche il funzionamento della macchina stessa, quindi...*
> *P.M. – No, ma mi scusi.* ***Lei nell'espletamento del suo incarico ha parlato solo con l'Avvocato o anche con l'indagato****?*
> *C.T. DIFESA – con entrambi.*
> *P.M. – Con entrambi. E quindi F. le ha indicato che è un programmatore?*
> *C.T. DIFESA– Eh, mi sembra sì, di aver ricordato questo tipo di informazione.*
> *P.M. – E* ***la macchina virtuale chi è che l'ha messa in piedi, lei o F.?***
> *C.T. DIFESA –* ***F., con me...***
> *P.M. – Scusi, lei attesta di avere messo in piedi una macchina virtuale, e poi dà anche dei giudizi sulla Polizia Giudiziaria ma in realtà poi la macchina virtuale l'ha messa in piedi l'indagato per lei? Nella sua integrazione dice "Ah, la Polizia Giudiziaria non è stata capace di mettere una macchina virtuale ed io l'ho messa su", perché la firma lei, ma invece è stato F. a mettere su la macchina virtuale?*
> *C.T. DIFESA – l'abbiamo fatto insieme.*
> *P.M. – prima aveva detto che è stato F., però?*
> *C.T. DIFESA – Sì, nel senso che l'ho fatta con F., non vuol dire che l'ho fatta da solo, per indicare il fatto che è stata un'operazione fatta insieme, è lì ho potuto anche rilevare in qualche la sua competenze. Quindi se lei mi chiede "Una persona normale usa questo sistema?", le dico "No", ma il F. non è un tecnico comunque comune.*
>
> *P.M. – Va bene. Un attaccante, numero 2, raggiunge la macchina M. con il servizio disponibile sulla macchina M. che, dopo vedremo, altri erano disponibili oltre a TeamViewer.*
> *C.T. DIFESA – Esattamente.*
> *P.M. – Però TeamViewer lei l'ha trovato?*
> *C.T. DIFESA –* ***TeamViewer era presente, certo.***

[57] Si noti che solo con memoria depositata il 15 maggio 2014 (all. 11) i difensori si lamentano dalla mancata corrispondenza degli hash, con verifiche eseguite il 2 maggio 2014 (in relazione ad un reperto consegnato il 18 settembre 2013).

[58] Si noti che solo con memoria depositata il 15 maggio 2014 (all. 8 quanto al NAS1-C) i difensori si lamentano dalla mancata corrispondenza degli hash, con verifiche eseguite il 2 maggio 2014 (in relazione ad un reperto consegnato il 18 settembre 2013).

*P.M. – lei parla sempre di **malware**, cioè il programma malevolo, però, per poi consentire anche nel contraddittorio della parti al Pubblico Ministero di fare considerazioni, questo tipo di malware non l'ha mai indicato né per esempio...*
C.T. DIFESA – Ma ad esempio...
P.M. – Aspetti, finisco la domanda.
C.T. DIFESA – Sì sì, scusi.
P.M. – Come capita in altri processi il Consulente trova la vulnerabilità, il malware, lo cristallizza e lo allega alla relazione, tutto questo non abbiamo trovato nella sua annotazione, c'è un motivo?
*C.T. DIFESA – Be', sì, **immaginavo che non fosse nella mia competenza dover spiegare che cosa facessero i malware**, ho solamente indicato...*
*P.M. – **No, la domanda è diversa**, malware eventualmente saranno le Parti a spiegarlo al Giudice se non lo conosce, però il concetto di malware è programma malevolo, ma io le chiedo: **perché non ha indicato compiutamente che tipi di malware ha trovato così e li ha cristallizzati in un Cd?** Così effettivamente anche il Pubblico Ministero poteva verificare se era effettivamente presente o meno. Cioè lei dice "Ho trovato un malware", ma non lo indica, non lo produce, non ne attesta l'operazione?*
*C.T. DIFESA – Ho comunque la risposta per lei, ovvero **il malware mi serviva per indicare solamente che la macchina fosse mal tenuta, ma la principale delle mie analisi è la Timeline,** non si deriva dal malware, la Timeline è stata realizzata con le attività fatte da qualcuno che si collegava da remoto e mi interessava poter dimostrare che negli orari in cui Proxpn dava un IP a F. non ci fosse attività o viceversa. Quindi il malware riportato è solamente...*
P.M. – Va bene, lei mi sta dando una risposta rispondendo ad altre domande. Le chiedo: ha documentato... cioè ho sbagliato io a non trovare nella sua annotazione, relazione di consulenza, il tipo di malware, le caratteristiche di questo malware?
C.T. DIFESA – non le ho documentate.

*P.M. – va bene. Allora, andiamo con ordine. Siamo a pagina 2 della sua annotazione. F., scrive, "Si collega ad una VPN ad orari determinati, non chiari dagli atti". Allora, la mia domanda è: ma scusi, **le tabelle non sono chiare nel riportare l'orario di collegamento al VPN?***
*C.T. DIFESA – Certo, sono chiare, **ma siccome ci sono due tabelle differenti, tra quella presentata il 18 settembre e quella di custodia cautelare, non sapevo bene quale considerare come riferimento, quindi le ho prese entrambe.***
P.M. – le rappresento, ma poi sarà motivo anche della discussione, che il Pubblico Ministero non è che si inventa le tabelle...
C.T. DIFESA – Non ho dubbi.
P.M. – Nel rappresentare i dati al Giudice fa riferimento agli atti dell'indagine, comunque non chiara agli atti in quel senso lì. E perché comunque li ha presi entrambi con il beneficio del dubbio?
*C.T. DIFESA – Perché **immaginavo che uno fosse giusto e l'altro potesse avere avuto degli errori di elaborazione e quindi non fosse giusto**. […]*



Linea dell'accusa che viene qui contestata

L'accusa ha ricostruito gli accessi al servizio Proxpn da parte dell'imputato.
Ha inoltre estratto una timeline di connessioni che l'ipotetico attaccante ha realizzato per collegarsi alla macchina del signor M[redacted] chiamata da qui in poi 'macchina M[redacted]'.

Negli atti a me consegnati dall'avvocato Veronelli, sono presenti due diverse tabelle che riportano gli orari, e questi orari differiscono tra loro. Ne copio qui di seguito l'evidenza.

- Sulla sinistra vediamo i log PROXPN riportato nell'atto "Relazione in merito dall'attività investigativa condotta sul PAT" del 18 Settembre 2012, Firmata da Garrisi.
- Sulla destra vediamo gli orari riportati nella richiesta di applicazione misura cautelare, con firma del dottor Cajani 5 Ottobre 2012, sempre relativi all'attività di F[redacted]i sul servizio PROXPN.

delfo2000@yahoo.it che si è collegato come segue:

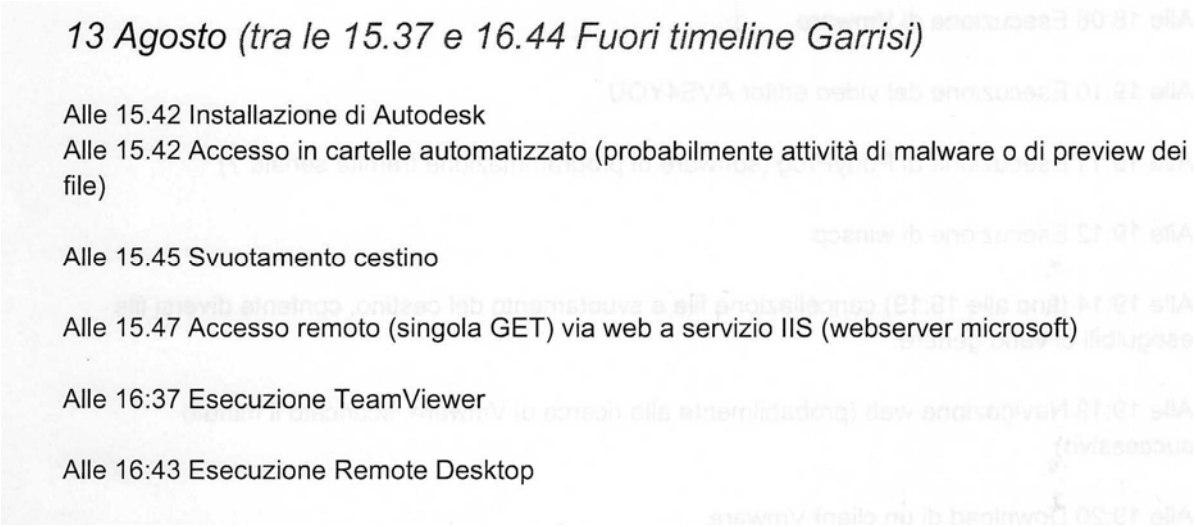
delfo2000@yahoo.it	8/13/2011 8:27	8/13/2011 10:16	85.88.202.118
delfo2000@yahoo.it	8/13/2011 13:09	8/13/2011 15:37	85.88.202.118
delfo2000@yahoo.it	8/13/2011 16:44	8/13/2011 20:31	85.88.202.118
delfo2000@yahoo.it	8/13/2011 21:02	8/13/2011 21:04	85.88.202.118
delfo2000@yahoo.it	8/13/2011 21:41	8/13/2011 22:24	85.88.202.118
delfo2000@yahoo.it	8/14/2011 5:08	8/14/2011 5:11	85.88.202.118
delfo2000@yahoo.it	8/14/2011 5:35	8/14/2011 6:36	85.88.202.118
delfo2000@yahoo.it	8/14/2011 8:05	8/14/2011 9:43	85.88.202.118
delfo2000@yahoo.it	8/14/2011 13:31	8/14/2011 15:58	85.88.202.118
delfo2000@yahoo.it	8/15/2011 5:32	8/15/2011 5:43	85.88.202.118
delfo2000@yahoo.it	8/15/2011 17:15	8/15/2011 17:22	85.88.202.118

CAPO A

delitto p. e p. artt. 81, 61 n. 11), 615-*ter* c.p. comma 1, 2 n. 3) e 3 c.p. perché, nella qualità di dipendente del Pio Albergo Trivulzio (PAT) e con abuso di relazione di ufficio, collegandosi – con la *user name delfo2000@yahoo.it* - ai servizi di anonimizzazione di PROXPN attraverso l'IP 85.38.202.118 (assegnato staticamente a[redacted]i dalla società Lineacom Srl), ottenendo a suo favore l' assegnazione dei seguenti IP ad opera di PROXPN

collegamento	*inizio*	*fine*	
13 ago 2011	*16.37*	*16.37*	213.179.212.76
13 ago 2011	*16.45*	*16.46*	213.179.212.76
13 ago 2011	*16.47*	*17.30*	213.179.212.76
13 ago 2011	*19.09*	*21.37*	109.203.115.89
13 ago 2011	*22.45*	*02.11*	109.203.115.71
14 ago 2011	*02.39*	*03.02*	213.179.212.122
14 ago 2011	*03.05*	*03.29*	173.231.157.74
14 ago 2011	*03.42*	*04.23*	109.203.115.66
14 ago 2011	*19.33*	*20.51*	109.203.115.109
14 ago 2011	*21.11*	*21.42*	109.203.115.109
14 ago 2011	*22.10*	*22.11*	213.179.212.70
14 ago 2011	*23.47*	*23.47*	213.179.212.69
15 ago 2011	*01.38*	*01.47*	173.0.5.51

P.M. – Allora, ***lei non ha verificato il fuso orario che Garrisi aveva indicato nelle tabelle?***
C.T. DIFESA – Sì, indicava meno 4, meno 5, non ben chiaro, giusto?
P.M. – no, lo legga, lo legga, gliel'ho...
C.T. DIFESA – Riferito ad un periodo che va dal 12 agosto 2011 al 15 agosto 2011 comunicando inoltre di non essere sicuro del fuso orario di riferimento, se è GMT meno 4 o meno 5, ma che comunque si trattava Eastern USA.
P.M. – e quindi ha tenuto quel fuso orario. Lo vede nella nota cosa dice?
*C.T. DIFESA – "****Pertanto si tratta di GMT meno 4 e così sono stati trattati i dati acquisiti", va bene****. Però qual è il punto? Che mi sono basato sulle tabelle di correlazione che erano già presenti su questi atti in cui si mettevano in corrispondenza l'attività dei log di Proxpn e le attività sulla macchina. Ho voluto partire da quella Timeline per dire "Vediamo se le date corrispondono". Comunque avevo specificato, anche al signor Giudice la volta scorsa, che può essere che le macchine come server online o anche la macchina stessa di M. avessero degli orari differenti, la cosa certa è che in fase di attacco...*
P.M. – Sì, ma appunto, è proprio qua che dobbiamo arrivare. Cioè non è che lei, prima di tutto a differenza di Garrisi, che lei critica, della Polizia Giudiziaria, che lei critica, le chiedo: ***quando nella sua Timeline mette l'orario a quale fuso orario vuole intendersi?***
C.T. DIFESA – ***Al fuso orario della macchina M.***
P.M. – ***Che sarà un fuso orario italiano****.*
C.T. DIFESA – ***Esattamente.***
P.M. – E allora non è che quando lei dice che alle 16.37 TeamViewer era eseguito e quindi è fuori dalla Timeline di Garrisi in realtà è dentro perché lei non ha tenuto conto del fuso orario che invece Garrisi aveva tenuto conto, e che guarda caso è meno due ore, e quindi alle 16.37 in realtà è alle 14.37?


13 Agosto (tra le 15.37 e 16.44 Fuori timeline Garrisi)

Alle 15.42 Installazione di Autodesk
Alle 15.42 Accesso in cartelle automatizzato (probabilmente attività di malware o di preview dei file)

Alle 15.45 Svuotamento cestino

Alle 15.47 Accesso remoto (singola GET) via web a servizio IIS (webserver microsoft)

Alle 16:37 Esecuzione TeamViewer

Alle 16:43 Esecuzione Remote Desktop

*C.T. DIFESA – **Li ho considerati comunque GMT più 2**, cioè allineati al fuso orario italiano, come anche la Polizia ha fatto quest'indagine spostando gli orari sommando 6 ore per allinearsi con l'orario italiano, anch'io ho fatto così basando sulla linea... ho copiato, eh? Cioè io i dati di Garrisi e i dati della custodia cautelare li ho copiati dagli atti cartacei.*
P.M. – Sì, ma nella tabella che lei dice di aver riprodotto, ma in realtà ne prende un'altra, c'è scritto che il fuso orario era GM(T) meno 4, giusto?
C.T. DIFESA – Sì sì, ho capito. Ora non ricordo sinceramente se lo presi da una tabella o dall'altra.
P.M. – Eh, ma caspita! Scusi un attimo, il Consulente dovrebbe introdurre elementi di certezza non ulteriori dubbi.
C.T. DIFESA – Okay, li ho presi dalla tabella della prima pagina.
P.M. – Nella tabella della prima pagina c'è la nota.
C.T. DIFESA – Uhm uhm, confermo.
*P.M. – E per altro **nell'annotazione di M. del 29 settembre, che le rimostro, si dice che "l'attaccato è avvenuto compromettendo il computer di M. utilizzando il programma TeamViewer a partire dal 13 agosto dalle ore 14.37 UTC circa sino al 15 agosto 2011 ore 11.14 UTC**". Quindi...*
GIUDICE – UTC che cosa vuol dire?
P.M. – l'orario del... è un orario, Universal Time Center[59], che poi deve essere portato sul fuso orario...
GIUDICE – Cioè è l'orario sfalsato di due ore in sostanza rispetto a noi.
GIUDICE – Deve essere portato all'orario italiano, e quindi...
C.T. DIFESA – qui è sfalsato di 6 ore e 10.
P.M. – Qui?
C.T. DIFESA – Qui è sfalsato di 6 ore e 10, cioè la connessione inizia alle 8.27, secondo questa tabella, e qui riportano le 14.37.
P.M. – No no no no, e sì che gli atti li aveva studiati bene. Da una parte è la tabella che parla dell'accesso a Proxpn.
C.T. DIFESA – Ah, okay, considerando gli attacchi, okay.
*P.M. – E lì invece solo TeamViewer. **Per cui quando lei dice "Ah, ma io non sapevo se TeamViewer l'avevano messo all'UTC o all'orario italiano", le dico che nell'analisi di M. la Polizia Giudiziaria dice che l'analisi... che TeamViewer è stato utilizzato a partire da un orario UTC ad un altro orario UTC, e inizia alle 14.37**. Io guardo la sua relazione e lei dice "**No, c'è un problema, perché io ho rilevato che il programma inizia alle 16.37", ma guarda caso sono giusto 2 ore in più, 14.37 UTC, 16.37 orario italiano**.*
Se lei avesse fatto la conversione era 14.37 dice Garrisi, […]. Sì o no?
C.T. DIFESA – mi sono un attimo perso sinceramente.

[59] **UTC – UNIVERSAL TIME COORDINATED:** il tempo coordinato universale, conosciuto anche come tempo civile e abbreviato con la sigla UTC (compromesso tra l'inglese Coordinated Universal Time e il francese Temps universel coordonné), è il fuso orario di riferimento da cui sono calcolati tutti gli altri fusi orari del mondo. Esso è derivato dal tempo medio di Greenwich (in inglese Greenwich Mean Time, GMT), con il quale coincide a meno di approssimazioni infinitesimali, e perciò talvolta è ancora chiamato **GMT** (tratto da wikipedia)

C.T. DIFESA – Sì sì, ho capito, ma allora quello che dovrei fare in questo momento è prendere i dati di quello che chiamo "Analisi Garrisi", spostarli di sei ore, e vedere che forme si rappresentano.
P.M. – no, ***lei doveva sincronizzare l'orario del computer che lei ha analizzato con quello invece dei dati di Garrisi****, visto che Garrisi fa riferimento a dei dati che ha ricevuto da Proxpn li ha già analizzati e le dà l'indicazione di orario.* ***Lei arriva e dice "No, attenzione, è tutto sbagliato perché le 16.37 è fuori dalla Timeline di Garrisi", le chiedo: ma non è che forse lei non ha sincronizzato la sua analisi con quella di Garrisi prima di fare le valutazioni?*** *Io dico, prima di fare le valutazioni, io sto ancora adesso analizzando sul suo metodo, sto facendo tutte domande sul suo metodo, quali atti ha ricevuto, se ha fatto da solo o con l'indagato, se ha fatto correttamente la conversione del fuso orario. Domande sul metodo del Consulente, perché, ripeto, poi dopo le Parti discuteranno sui risultati. Quindi visto che alla Procura e alla Polizia Giudiziaria interessava TeamViewer, e lei dice "Attenzione TeamViewer è 16.37", le rifaccio la domanda perché è chiaro al Giudice però io vorrei una risposta se sì o no: lei ritiene di aver fatto correttamente la conversazione del fuso orario e quindi questa discrepanza che lei ha rilevato è rimproverabile ad un suo errore di metodo, sì o no?*
C.T. DIFESA – a dire il vero la mia analisi doveva riuscire a sopperire anche ad eventuali errori di localizzazione nella tempistica, perché mi ero molto... faccio molto affidamento sul fatto che se anche ci fossero stati orari differenti... fusi orari differenti le forme che rappresentano i momenti in cui c'erano un tipo di attività e l'altra attività combaciassero spostate ma...
P.M. – la domanda è semplice. Su TeamViewer, che era uno degli elementi fondamentali, poi le farò altre domande e l'Avvocato può fare le altre domande sul resto, però io le dico, su questa discrepanza, che guarda caso evidenzia TeamViewer fuori dalla Timeline della Polizia Giudiziaria, ***le ripeto per la terza volta e deve rispondere o sì o no****, forse è un suo errore di metodo che non ha correttamente sincronizzato il fuso orario della sua analisi orario italiano con il fuso orario di Garrisi?*
C.T. DIFESA – prima di risponderle, in cui naturalmente è evidente che possa aver fatto un errore di localizzazione del tempo, va detto che TeamViewer è eseguito alle 16.37, mentre qui si sta parlando di orari che inizierebbero alle otto di mattina, che anche sommandoci 6 ore arriveremmo alle 14.00.
P.M. – Le ripeto, Dottor …. lei ha analizzato gli atti e non può dire che quella annotazione fa riferimento a TeamViewer, perché quella annotazione a cui lei fa riferimento fa riferimento all'accesso alla Proxpn, l'annotazione a cui fa riferimento a TeamViewer è l'altra che lei ha sotto occhio, se è la prima volta che la vede mi dispiace per il Consulente, però in quella annotazione si dice che l'orario di TeamViewer è dalle 14.37 UTC, quella è il suo atto di riferimento.
C.T. DIFESA – ho capito, eh...
P.M. – ***c'è un errore, sì o no, di metodo?***
C.T. DIFESA – ***sì.***

Orbene, è il consulente della Difesa ad ammettere di fronte al giudice l'errore di metodo nel quale è incorso….

Nell'immagine qui sotto è nuovamente riportato l'estratto dei log di ProXPN in cui si evidenziava, ad opera della polizia postale (Garrisi), la data in orario EDT[60] (GMT –4).

delfo2000@yahoo.it	8/13/2011 13:09	8/13/2011 15:37	85.88.202.118

Confrontando quanto appena detto con l'altra immagine qui sotto riportata – in cui vengono riportati tutti gli orari in LOCAL TIME[61] (GMT +2) – appare chiaro come da EDT (GMT –4) a LOCAL TIME (GMT +2) passano 6 ore.

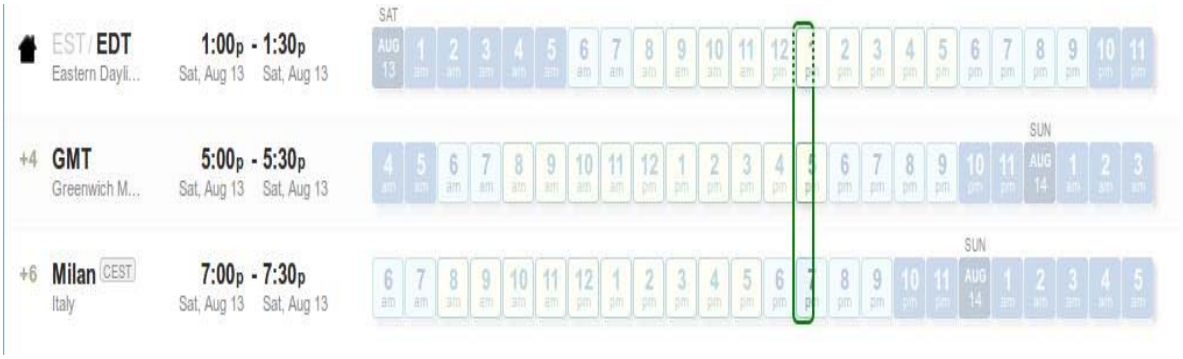
Il risultato è la tabella di seguito[4]:

mail	Inizio connessione al servizio VPN	Fine connessione al servizio VPN	Inizio connessione/i con Team Viewer	Fine connessione/i con Team Viewer	Ip utilizzato per la connessione/i
delfo2000@yahoo.it	8/13/2011 19:09	8/13/2011 21:37	19.09 13/08/2011	21.37 13/08/2011	109.203.115.89

[60] Eastern Daylight Time.

[61] Fuso orario italiano.

Per comprendere al meglio la localizzazione oraria, si veda la figura qui sotto in cui sono messi in successione i tre fusi orari nella data del 13 agosto 2011:



Il consulente tecnico dell'imputato quindi erra nella conversione dei fusi orari, dal momento che prende in considerazione orari intendendoli in formato LOCAL TIME (GMT+2) mentre in realtà erano in formato UTC (GMT), con differenza quindi di 2 ore in meno (con la conseguenza che Team Viewer viene dallo stesso consulente indicato attivo alle ore 16.37 mentre in realtà, come da sempre sostenuto dalla polizia giudiziaria, erano le 14.37).

P.M. – Va bene. Allora passerei, sono le ultime domande, alla terza sua annotazione, "Contestazione dell'integrità della prova". Allora, qui lei dice, e lo indica anche, qui non c'è bisogno di integrazione sul metodo, di avere analizzato ***il disco del computer di M.*** *con l'indicazione, che è la stessa che ricava della Polizia Giudiziaria.*
[…]
P.M. – Però ***poi dopo dice di aver ritrovato un'anomalia****.*
C.T. DIFESA– Esattamente.
P.M. – E dà tre ipotesi di quest'anomalia. Io vorrei avere delle integrazioni sempre di metodo sulla seconda ipotesi. Cioè lei dice "Il checksum, quindi la firma, il controllo della firma è valido".
C.T. DIFESA – Anche l'ipotesi... non è plausibile?
P.M. – Guardi glielo direi con facilità se...
C.T. DIFESA – Sì sì, ce l'ho qui davanti, anche l'ipotesi...
P.M. – 2 e 3, alla pagina 4. Dà quest'ipotesi, cioè dice che l'attività di Polizia Giudiziaria è – mi dica, sintetizzo anche per il Giudice – è corretta.
C.T. DIFESA – Sì.
P.M. – ***L'attaccante ha utilizzato alcuni programmi per nascondere e sporcare le tracce e così facendo ha modificato o manipolato le date e gli accessi da alcuni settori, perché lei dice "Non è possibile che io ritrovo un file che la data successiva a quello della firma", è così?***
C.T. DIFESA – non proprio. Nel senso che è possibile trovare un file che abbia la data successiva, ma non è possibile trovare che delle directory in questo modo sequenziale vengano cedute nell'arco di pochi secondi, in questo caso 75 secondi.
P.M. – ***e fa la sua valutazione, "In tal caso (estremamente poco plausibile) le intere analisi effettuate sull'hard disk M. vanno considerate compromesse perché l'attaccante avrebbe manipolato anche i dati in mano ad Accusa e Difesa".***
C.T. DIFESA – Sì, sono giusto delle ipotesi per dire "Davanti a questa anomalia che cosa possiamo fare?".
P.M. – ***ma lei ha letto attentamente la nota di Garrisi del 29 settembre 2011, dove la Polizia Giudiziaria dice proprio questo?***
C.T. DIFESA – ***temo che si parli di cose differenti*** *perché penso di Garrisi...*
P.M. – Allora, leggiamola insieme, così mi dà la sua interpretazione.
C.T. DIFESA – "Visto quanto sopra si analizzava che c'erano tracce di cancellazione non usuali, cestino, l'analisi permetteva di trovare all'interno di parti non allocati del disco parti dei log originali del programma TeamViewer dai quali ricostruiti si evince l'attacco, eccetera". Ho capito infatti questo qui è quello che si considera il... abbiamo trovato un log nella parte non allocata del disco. Quello che mi interessava però...
P.M. – Ascolti, però le faccio la domanda perché io voglio capire quale lettura lei ha dato agli atti di Polizia Giudiziaria prima di fare le sue considerazioni. Cioè mi deve confermare, perché ***a me sembra che la Polizia Giudiziaria dice "Abbiamo analizzato il computer di M., ci siamo accorti che era molto compromesso, e quindi abbiamo analizzato dei file di log in una parte non allocata, cioè così nascosta che non poteva verosimilmente essere compromessa, e solo questo poi portiamo all'attenzione del Pubblico Ministero e non tutto il resto", lei così l'ha intesa come l'ha intesa il Pubblico Ministero o l'ha intesa in una maniera diversa?***
C.T. DIFESA – ***A dire il vero sì, ho inteso che questo mi ha comunicato la Polizia****, ho inteso che hanno trovato una parte di file residua da una cancellazione o da uno spostamento.*

P.M. – che sono proprio i file di TeamViewer, che lei dice "Non ho neanche analizzato".
C.T. DIFESA – Sì, ma ho visto quella parte del (Inc.) non l'ho riportato sulle relazioni perché quello che c'era sulle relazioni della Polizia era coerente con quello che ho guardato io. Il punto è che quello che mettevo in discussione non è il fatto che un file possa avere una data nel futuro e che l'unica possibilità per cui si abbia un cambio di date a 6 giorni di distanza in directory sequenziali, una dopo dell'altra, è che l'hard disk è stato attaccato in scrittura ad un computer e questo computer in modo automatico con antivirus piuttosto che con una preview dei file ha iniziato ad accedere a questi file modificando la data.
P.M. – ***Ma non può essere che l'attaccante, ipotesi che lei esclude, però mi deve spiegare perché, abbia volutamente modificato le tracce****, perché poi dopo lei dà ipotesi A) e dice "Questo tuttavia non è contemplato nelle indagini"; ipotesi B), quella che per altro è fatta proprio alla Polizia Giudiziaria, dice "Estremamente poco plausibile", ipotesi C), che io credo lei validi, perché dice "In questo caso la prova dovrebbe essere invalidata". Quindi a me sembra che lei, anche se non si esprime in questo passaggio a mio parere in maniera cara, dice "Secondo me l'ipotesi più verosimile è al numero 3", ho interpretato bene?*
C.T. DIFESA– No no, anche per me è più verosimile, solo che siccome mi sembra... cioè siccome la catena di custodia era mantenuta valida non mi sembrava fosse la considerazione più sensata.
P.M. – Sì, ho capito, ma lei, cioè nel senso, cioè come Consulente può anche dare delle sue valutazioni, ripeto, però a me sembra che lei dica "La prima non è contemplata dalle indagini, la seconda è estremamente poco plausibile, e la terza invece è quella che io valido", però sulla seconda le dico "Ma lei non si è accorto che la Polizia Giudiziaria dice "Noi abbiamo visto l'hard disk come l'ha visto lei, abbiamo visto che era compromesso, l'abbiamo acquisito, ma abbiamo valutato a fine d'indagine un unico dato, cioè quello che era rimasto in una parte non allocata e quindi difficilmente poteva essere stato modificato come tutto il resto, cioè questa parte lei l'ha compresa e...
C.T. DIFESA – Ma certo.
P.M. – E quindi mi dice come, ***su quali dati il suo giudizio di estrema, poco plausibilità si fonda? Su quali dati si fonda se è la stessa Polizia Giudiziaria che dice questa cosa qua.***
C.T. DIFESA – Perché la modifica che ho rilevato, che le ho prodotto in questa relazione, non riguarda il fatto che un file è stato cancellato o sporcato, riguarda il fatto che ci sono 75 secondi 6 giorni dopo l'acquisizione che non dovrebbe esserci, e ***questo tipo di compromissione non l'ho mai visto in nessun sistema di occultazione che viene utilizzato dagli attaccanti****, non l'ho mai visto come meccanismo utilizzato per sporcare una prova, quindi mi sembra proprio un cattivo utilizzo del dispositivo o comunque un utilizzo in scrittura del dispositivo dopo l'acquisizione.*
P.M. – E questo passaggio che lei indica dov'è? Visto che poi ha fatto un copia e incolla... di 1, 2, 3, 4, 5, 6, 7, 8, 9...
C.T. DIFESA – Quel copia incolla sono gli accessi...
P.M. – Sì, ma dov'è questo passaggio, così lo possiamo vedere anche noi e poi fare le nostre valutazioni in sede di discussione, dov'è questo passaggio che lei non ha mai visto? Cioè dove sono i dati di questo passaggio?
C.T. DIFESA – Vede queste... la parte che ho incollato?
P.M. – sì.
C.T. DIFESA – Dimostrano che sono sati degli accessi automatici dalle 10.31 del 24 agosto.
P.M. – Dalle 10.31 del 24 agosto fino?
C.T. DIFESA – Mi ricordavo 75 secondi, ora... fino a...
P.M. – Quindi...
C.T. DIFESA – Il 24 agosto 10.31.35.
P.M. – Quindi sulla base della sua esperienza, se così possiamo chiudere, mi sembra di capire che lei si potrebbe immaginare l'azione dell'attaccante che sporca l'hard disk?
C.T. DIFESA – No no, questo qui immagino che non sia l'azione dell'attaccante, questo immagino che sia l'azione di un hard disk che abbiamo collegato senza blocchi di scrittura ad un computer.
P.M. – Sì, ma non può essere invece l'azione dell'attaccante che sporca con metodi automatizzati l'hard disk?
C.T. DIFESA – A 6 giorni di distanza no, non credo.
P.M. – No, a sei giorni di distanza no, perché potrebbe anche aver spostato l'orologio di 6 giorni e quindi in quel momento lì.
C.T. DIFESA – ***Be', ma non darebbe un comportamento simile, questo qui è il comportamento proprio di quando un antivirus inizia a scansire le directory, cambia invece.***
P.M. – ***Ma lei ha trovato dentro alla macchina di M. un antivirus che potrebbe fare questa cosa?***
C.T. DIFESA – No no.

A commento di quest'ultimo tentativo difensivo, occorre ricordare – come già sostenuto in altre occasioni – che pare condivisibile l'impostazione tecnica di chi ritiene che "la possibilità della modifica di una successione di bit andrebbe presuntivamente considerata come avvenuta, con la conseguenza che, qualora in un procedimento venisse prodotto in giudizio un dato informatico, lo stesso andrebbe presuntivamente considerato come modificato ad arte, dovendo la parte interessata alla sua acquisizione nel processo dimostrarne l'attendibilità. Tuttavia, la presunzione di ripudio non andrebbe intesa come una dichiarazione di inattendibilità del dato informatico, in quanto tale considerazione verrebbe facilmente contraddetta dall'esistenza della stessa firma digitale. Ugualmente, la presunzione di ripudio del dato informatico non deve far pensare che il dato informatico sia inutilmente entrato nel processo, bensì deve essere percepita nel senso

che la parte che produca un dato informatico sia onerata dalla dimostrazione della genuinità e attendibilità del dato stesso"[62].

E pur tuttavia, occorre ancora una volta riaffermare come l'onere probatorio in capo all'organo dell'accusa potrà considerarsi correttamente assolto nel momento in cui venga indicato, per l'istruttoria dibattimentale:

- da chi sia stato individuato il dato informatico;
- come tale dato si presentava al momento della sua individuazione ad opera della parte (ufficiale di polizia giudiziaria, persona offesa, terzi non aventi alcun minimo interesse ai fatti di cui al processo [63]),
- con quale modalità e dopo quanto tempo tale persona lo abbia acquisito;
- in che modo siano state successivamente conservate le "sue caratteristiche oggettive di qualità, sicurezza, integrità" (prendendo a prestito l'efficace dizione normativa di cui all'art. 21 comma 1 D.lgs. 82/2005), così come presenti al momento della individuazione/acquisizione.

Spetterà a quel punto alla difesa dimostrare il contrario, non in termini generali ed astratti – come avvenuto nel caso in esame, e peraltro con un errore metodologico quanto alle evidenze di Team Viever – ma semmai indicando gli elementi, anche acquisiti a seguito di indagini difensive, che dimostrino come nel caso concreto il processo di individuazione/acquisizione/conservazione del dato informatico, così come rappresentato in dibattimento dall'accusa, abbia invece portato ad una alterazione dello stesso, tale da inficiarne un giudizio di attendibilità probatoria.

Sul punto invece l'imputato, in uno coi suoi difensori e consulente tecnico, non ha fatto altro che riferirsi ad ipotesi teoriche ovvero, per indicarle negli stessi termini dell'imputato[64], a "mere invenzioni" (frutto di un erronea comprensione degli atti di indagine).

Anche sotto tale ottica, la motivazione del tribunale di Bologna sul caso Vierika[65] appare – anche a seguito delle innovazioni *ex* legge n. 48 del 2008 – ancora condivisibile laddove indica che non sia compito del "Tribunale determinare un protocollo relativo alle procedure informatiche forensi, ma semmai verificare se il metodo utilizzato dalla p.g. nel caso in esame abbia concretamente alterato alcuni dei dati ricercati. In altre parole, non è permesso al Tribunale escludere a priori i risultati di una tecnica informatica utilizzata a fini forensi solo perché alcune fonti ritengono ve ne siano di più scientificamente corrette, in assenza della allegazione di fatti che suggeriscano che si possa essere astrattamente verificata nel caso concreto una qualsiasi forma di alterazione dei dati e senza che venga indicata la fase delle procedure durante la quale si ritiene essere avvenuta la possibile alterazione".

---

[62] D. CACCAVELLA, *Gli accertamenti tecnici in ambito informatico e telematico* in S. ATERNO, P. MAZZOTTA, *La perizia e la consulenza tecnica*, Padova, 2006, 198.

[63] la cui testimonianza nel processo potrà essere valuta dal giudice con un maggiore grado di attendibilità, in astratto, rispetto a quanto potrebbe invece rappresentare la persona offesa.

[64] Cfr. spontanee dichiarazioni dell'imputato all'udienza 8.7.2013, p. 181:

IMP. – Visto quello che ho sentito io avrei moltissime cose soprattutto nell'aspetto tecnico da ribadire, anche perché ***molte le ho trovate delle mere invenzioni per non dire dei salti logici anche in mala fede a mio avviso****, però mi riservo di avere anche l'opinione del mio Consulente Tecnico. Solo questo volevo sottolineare.*

[65] Il riferimento è a tribunale di Bologna, Sez. I mon. pen, sentenza 1823/2005, in *Dir. Internet*, 2006, f. 2, 153 ss. con nota di L. LUPARIA, *I profili processuali*. Per il testo integrale della sentenza cfr. *http://www.penale.it/page.asp?mode=1&IDPag=182.*

CASO PRATICO N. 10

Una telefonata poco prima dell'accesso ad una 'wifi bucata'

a cura di F. CAJANI

Cap. 7 – L'ACQUISIZIONE DEI DATI DEL TRAFFICO
PARTE II: TABULATI TELEFONICI E LOG FILES
Par. 1: Tabulati telefonici e log files come irrinunciabili spunti investigativi ed importanti fonti di prova

Un triangolo amoroso: lei (AA), lui (BB) e l'altro (CC).

Quando lui scopre che lei ha un altro, si lasciano.

Lei poi ritorna con lui, ma una mattina i due ricevono una e-mail apparentemente proveniente dall'altro: con allegati una serie di conversazioni (decisamente intime e senza pudore) intrattenute dai due via posta elettronica e relative alla loro passata relazione amorosa. Una e-mail che però raggiunge molti colleghi della persona offesa, con enorme pregiudizio per la stessa.

A questo punto lei querela il suo ex, allegando il testo della e-mail ricevuta.

Un caso apparentemente già risolto.

Vale la pena di riportare per esteso le relative annotazioni di indagine, redatte da Ufficiali di polizia giudiziaria[1] con una solida impostazione investigativa "classica" ma non per questo meno attenti ai temi delle tracce digitali che si possono individuare presso la *scena criminis*.

Con un risultato a sorpresa, sicuramente merito del fiuto investigativo e di una buona dose di ostinazione nel cercarlo.

> […] la parte lesa **AA**, deposita la querela nei confronti di **CC**, ritenendolo responsabile dei reati di cui agli artt. 594, 595 e 615ter del C.P.
>
> La denunciante, sostanzialmente, riferisce che dopo aver conosciuto nel mese di gennaio 2007 il **CC** in occasione di vacanza all'estero in compagnia del proprio fidanzato BB, al rientro in Italia, intraprese con il **CC** una relazione sentimentale ed anche una collaborazione professionale in attività imprenditoriale nell'ambito […], settore ove già quest'ultimo operava. Detta collaborazione professionale si interrompeva, però, verso la fine dello stesso anno per incomprensioni di carattere gestionale ed operativo.
>
> La decisione di interrompere la relazione sentimentale e contemporaneamente anche quella professionale, non sarebbe stata condivisa dal **CC** che avrebbe, quindi, maturato un certo rancore al riguardo. La denunciante riferisce che nel pomeriggio del giorno **8 agosto 2008**, aveva avuto modo di leggere una e-mail inviatale il giorno precedente ai propri indirizzi di posta elettronica *aa@hotmail.com* e *aa@tiscali.it* dal **CC**, dal contenuto diffamatorio ed offensivo nei confronti della medesima.
>
> Sempre la parte lesa riferisce anche che detto comunicazione telematica diffamatoria sarebbe stata inviata anche a docenti/dipendenti della università […]. Infatti la stessa, soggiunge anche di essere stata contattata da questi ultimi che le segnalavano a loro volta l'avvenuta ricezione del messaggio di posta elettronica come destinatari per conoscenza in copia nascosta. La stessa, comunque, per scrupolo, aveva contattato coloro che avevano ricevuto la mail i quali confermavano che il testo era identico per tutti.

[1] M.A. CC. Giuseppe Acacia e Lgt. CC. Nicola Tragni (all'epoca in forza alla Sezione di polizia giudiziaria – aliquota Carabinieri della Procura di Milano).

La circostanza che la **AA** era ed è dipendente dell'università […], risultava nota al **CC**, anche in considerazione che la parte lesa avrebbe avuto modo di fargli conoscere personale docente e non dello stesso ateneo.
Per ultimo, tra l'altro, la parte lesa accusa il **CC** di aver acquisito in maniera fraudolenta la rubrica dei propri contatti di posta elettronica detenuti sul proprio personal computer. Inoltre, nel mese di marzo 2008, la parte lesa non sarebbe più riuscita ad utilizzare il proprio indirizzo di posta elettronica *aa@hotmail.com* per un accesso abusivo di utente sconosciuto così come comunicatole dal provider di riferimento Hotmail.

[…] la S.V. Delega gli scriventi al compimento di ogni accertamento utile alla prosecuzione delle indagini ed alla individuazione del responsabile.

Come consuetudine, questa PG preliminarmente ha ritenuto opportuno convocare […] la parte lesa per chiarire più dettagliatamente i termini della vicenda. L'interessata presso questi uffici ha, in sintesi, riferito quanto segue [all.to 1]:
1. ha confermato di aver ricevuto il messaggio di posta elettronica diffamatoria su entrambi i suoi indirizzi mail: *aa@hotmail.com* e *aa@tiscali.it*;
2. ha precisato che le erano state sottratte ambedue le caselle di posta elettronica, intendendo con ciò che, nel periodo successivo al mese di aprile 2008, non è più riuscita a collegarsi con dette caselle di posta elettronica;
3. anche in tale sede ha indicato e confermato gli indirizzi di posta elettronica/telefonici degli altri destinatari della medesima e-mail, dichiarandosi disponibile, a specifica richiesta degli scriventi, all'acquisizione del messaggio in argomento su ambedue gli indirizzi di posta elettronica.

Vista la disponibilità palesata dalla parte lesa […] veniva effettuata l'acquisizione della mail diffamatoria ricevuta sull'indirizzo *aa@hotmail.com* [all.to 2]. Tale acquisizione è stata eseguita tramite collegamento alla Webmail direttamente dal PC in carico a questo ufficio.
In data […] veniva, invece, eseguita l'acquisizione dello stesso messaggio diffamatorio giunto all'indirizzo *aa@tiscali.it* [all.to 3]. Operazione questa eseguita direttamente sul PC portatile della parte lesa in quanto, per tale casella di posta, la stessa utilizzava il client "Incredimail Xe" e, quindi, il messaggio si trovava salvato in locale.
Le acquisizioni erano necessarie al fine di poter visionare gli **header** che generalmente vengono nascosti all'utente e nei quali vengono conservati i dati relativi ai vari passaggi telematici indispensabili all'invio ed alla ricezione della posta elettronica. Tale attività tecnica ha permesso di stabilire inequivocabilmente che il messaggio era del tutto identico nella parte visibile all'utente ed inviato ai due indirizzi della parte lesa (uno direttamente *aa@tiscali.it* e l'altro per copia conforme *aa@hotmail.com*). Non risultano ulteriori destinatari ma risulta inviato dallo stesso mittente, ovvero *cc@fastwebnet.it*.
Dall'esame dell'header nascosto del messaggio ricevuto dall'indirizzo *cc@tiscali.it* risulta quanto segue:
– campo FROM: (mittente del messaggio) *cc@fastwebnet.it*;
– campo TO: (destinatario diretto) *aa@tiscali.it*;
– campo CC: (destinatario per copia conforme) *aa@hotmail.com*;
– campo Subject: (oggetto del messaggio) RE: scuse;
– campo Date: (data del messaggio) Thu, 7 Aug 2008 07:12:45 +0200;
– campo X-Mailer: (client di posta utilizzato) Microsoft Outlook Express 6.00.2900.2180.
Fin qui i dati relativi alla mail inseriti direttamente dal client di posta utilizzato che come è specificato nel campo X-Mailer, è L'Outlook Express versione 6.

Ancora di seguito e sempre relativamente allo stesso messaggio, si evidenziano le *tracce* che lasciano i vari server che si occupano dell'inoltro e smistamento delle mail:
– Received: from aa012msr.fastwebnet.it (85.18.95.72) by mail-mx-4.tiscali.it (8.0.016) id 489A972B0017EA1F; Thu, 7 Aug 2008 17:45:58 +0200;

– Received: from CC[2] (1.18.54.161) by aa012msr.fastwebnet.it (8.0.013.5) id 4889F7DF01A02E8E; Thu, 7 Aug 2008 17:45:56 +0200.
Per convenzione ogni server interessato alla *lavorazione* del messaggio di posta elettronica inserisce una sua riga con le proprie specifiche[3]. Proprio perciò i dati sopra riportati vanno letti in senso contrario (dal basso verso l'alto) in quanto ognuno dei server inserisce –in maniera conseguenziale– la propria riga di informazioni in testa all'header già presente.

Dalla lettura dei due *Received* si nota come un HOST denominato CC invia il messaggio di posta elettronica al server di fastweb che successivamente lo trasmette a quello di tiscali. Viene perciò rilevato l'indirizzo IP con il quale viene effettuata la trasmissione a tiscali **85.18.95.72**. Dall'accertamento Whois su tale indirizzo è risultato gestito dalla società FASTWEB, per cui, con annotazione [….], veniva richiesta l'emissione di apposito provvedimento per l'acquisizione dei files di log relativi al predetto IP. Provvedimento trasmesso per l'esecuzione […] [all.to 4].
[….] Fastweb, in merito al provvedimento, risponde che l'indirizzo IP *non risulta intestato ad alcun cliente ma risulta associato ad apparato interno alla rete fastweb* [all.to 5]. La risposta ricevuta, in considerazione del fatto che la rete di Fastweb è nattata[4], ha indotto gli scriventi a rivedere la lettura delle due righe *Received* dell'header. Rilettura che ha portato a considerare l'indirizzo IP strettamente collegato con l'HOST e dal quale viene inviato il messaggio al server di fastweb; cioè quello riferibile all'HOST CC. Tale indirizzo è **1.18.54.161**.
[…] quindi, si ritorna in argomento con Fastweb richiedendo l'anagrafica completa del cliente, collegato all'IP sopra detto, della loro rete interna [all.to 6]. A tale richiesta, sotto la stessa data, Fastweb ci comunica in merito all'indirizzo IP **1.18.54.161** [all.to 7]:
– ***vi comunichiamo che tale indirizzo IP risulta intestato a XY, presso Milano – via Farini Carlo, 3x, C.F. […], titolare di un contratto fastweb attivo dal […]. Indirizzo mail associato all'utenza:*** *xy@fastwebnet.it*.

Contrariamente a quanto appariva pacifico emergere dalla mera lettura dell'header (quello inserito automaticamente dal client di posta elettronica), quest'ultimo inconfutabile dato fornitoci da Fastweb ci portava a riconsiderare l'*identificazione* ormai verosimilmente certa del mittente, tanto da indirizzare la nostra attenzione sulla persona di XY, persona, fino a questo momento, completamente sconosciuta all'attività di indagine e tanto meno presente in atti al procedimento. Conseguentemente, si giunge poi alla necessità di acquisire l'anagrafica completa del reale intestatario della casella di posta elettronica *cc@fastwebnet.it*. A ciò […] Fastweb risponde:
– **tale casella e-mail risulta intestata a CC, presso** [….] **Milano, […], titolare di un contratto FASTWEB attivo dal […]. L'utente ha a disposizione per la navigazione gli indirizzi IP interni alla rete Fastweb dal 1.67.86.73 al 1.67.86.77** [all.to 8].
Da ciò ne deriva che la casella di posta elettronica *cc@fastwebnet.it* è effettivamente intestato all'indagato. Ma è, altresì, chiaro che la mail diffamatoria non è stata inviata da alcuno degli indirizzi IP assegnato e nella disponibilità dello stesso.
Stante l'evidente discrasia dei dati fin qui acquisiti, si richiedono nuovi e più compiuti chiarimenti a Fastweb relativamente ai due *Received* dell'header del messaggio in argomento. In data […] il provider comunica [all.to 9]:
– **"Received: from CC (1.18.54.161)": il nome "CC" è riferito all'Host name (nome della macchina/pc utilizzato); La e-mail è stata inviata dall'indirizzo IP 1.18.54.161 assegnato in maniera**

[2] Si trattava del cognome di CC (ndr.)

[3] Le specifiche inserite dai server sono: nome del PC che invia la mail in origine (HOST), indirizzo IP assegnato allo stesso, server a cui viene inoltrato il messaggio, indicazione del gruppo data/orario nonché del fuso orario di riferimento

[4] Con il termine nattata si intende una rete gestita tramite N.A.T. (Network Address Translation). Nello specifico ciò significa che ad un singolo indirizzo IP pubblico, tramite un router, possono essere collegati contemporaneamente diversi utenti, con ciascuno un proprio indirizzo IP interno alla rete creata dal router.

univoca alla sig.ra XY, via Farini Carlo, 3x Milano, […] titolare di un contratto FASTWEB attivo dal […];
– **"Received: from aa012msr.fastwebnet.it (85.18.95.72) by mail-mx-4.tiscali.it (8.06.016)": La e-mail è stata inviata dall'IP 1.18.54.161 attraverso il Mail Server FASTWEB con indirizzo 85.18.95.72 verso un indirizzo e-mail tiscali (by mail-mx-4.tiscali.it)**.
Da una ennesima ed ancor più approfondita lettura dell'header del messaggio diffamatorio si nota una considerevole differenza di orario tra quello posto dal client "Microsoft Outlook 6" (Thu, 7 Aug 2008 07:12:45 +0200) e quello inserito dal server di Fastweb (Thu, 7 Aug 2008 17:45:56 +0200). Considerato che l'orario reale non può che essere quello inserito dai server interessati alla *lavorazione* della e-mail, ritenendo che sia impossibile, se non a causa di problemi tecnici, che trascorrano circa 10 ore dall'invio del client alla ricezione del primo server, sono stati richiesti chiarimenti, anche in questo caso, a Fastweb. In data […], a tale proposito, si otteneva la seguente risposta [all.to 10]:
– **vi precisiamo che il gruppo data orario del corpo del messaggio è un dato configurabile dal client dell'utente; inoltre, in data 7 agosto 2008 non risultano esserci stati problemi o sospensioni nell'erogazione del servizio di invio/ricezione mail sui mail server FASTWEB.**

A riguardo dell'altra mail acquisita e relativa all'altro indirizzo della **AA**, *aa@hotmail.com*, si rappresenta che mostra le stesse identiche caratteristiche tecniche con unica differenza per il server che per ultimo riceve il messaggio che naturalmente è quello di "Hotmail bay0-mc11-f5.bay0.hotmail.com". Si fa notare che risultano, altresì, identici gli orari di spedizione da parte di Fastweb e di ricezione da parte di Hotmail rispetto a Tiscali.

Posto ciò, emerso in maniera inequivocabile il dato oggettivo del differente reale mittente della mail in argomento (XY e non CC), questa PG ha ritenuto indispensabile convocare XY presso questi uffici per acquisire ulteriori chiarimenti della vicenda.
La stessa in sede di sommarie informazioni, ha riferito sinteticamente quanto segue [all.to 11]:
– è titolare da circa dieci anni di contratto con Fastweb; anche ADSL da solo cinque anni;
– di non conoscere né **CC**, né **BB** né, tantomeno, **AA**. Ha anche specificato di non aver mai avuto rapporti di alcun genere con l'università […].

Nella circostanza, considerando che la teste era stata accompagnata dal coniuge YX, gli scriventi hanno ritenuto utile assumere ulteriori informazioni anche da questi. Il predetto ha riferito, sinteticamente, quanto segue [all.to 12]:
– di essere stato dirigente di una società americana che si occupa di information technology;
– ha confermato che dall'anno 2004, hanno installato in casa una linea Fastweb con abilitazione dell'ADSL per Internet;
– che la linea ADSL è gestita da un router del tipo wireless al quale si sono collegati, nel tempo, i tre PC che ha avuto a disposizione;
– da qualche mese ha sostituito il vecchio router con uno nuovo della Apple e, soltanto dal mese di luglio di quest'anno, ha predisposto la messa in sicurezza della rete wireless per mezzo di chiave di criptazione WPA. Quindi, fino a luglio u.s., la rete era totalmente aperta e lo stesso non aveva abitudine di spegnere il router;
– ha specificato di non conoscere il **CC**, né **BB**, così come la **AA**.

L'esito dell'attività di indagine sopra descritta, ci consente di poter ragionevolmente affermare che colui che ha effettivamente inviato la mail diffamatoria, ha approfittato del libero accesso della rete wireless riconducibile – in questo caso – alla XY. V'è da dire che appare singolare ma anche illogica, che il **CC**, per inviare tale mail, si adoperi prima nella ricerca di una rete wireless priva di protezione, la utilizzi poi inviando l'e-mail non con identità di comodo ma con la propria, esponendosi così a conseguenze anche di carattere penale come nel caso di specie.

A tal proposito, si segnala qualora non già noto, che esiste la possibilità di approntare una e-mail con i dati (che poi appaiono visibili a chi la riceve) falsati, ovvero: il mittente, il gruppo data/orario e finanche il tipo di client di posta utilizzato, tutti diversi da quelli reali.
È, infatti, possibile farlo con varie metodologie tra le quali, quella più semplice potrebbe essere quella di creare un account di comodo e temporaneo sul client Outlook Express. Metodo questo per cui si può assegnare il nominativo all'account (che poi sarà quello che apparirà come nome HOST) ed anche l'indirizzo di posta elettronica. Nella creazione di tale account si avrà cura di inserire la user-name che corrisponde all'indirizzo di posta elettronica e la password che, come sarà specificato di seguito, può essere anche di comodo. A questo punto rimane indispensabile, tenendo conto che la maggior parte degli ISP (Internet Service Providers) fa un controllo solo sulla parte dominio dell'indirizzo di posta, trovare una rete non protetta conforme al dominio dell'indirizzo che si vuole utilizzare, in questo caso Fastweb.
Il funzionamento dei mail-server per l'invio (SMTP), diversamente da quello per la lettura (POP3), non prevede autenticazione in quanto dà per scontato di averla già acquisita all'atto della connessione alla rete.
Nel caso di specie, infatti, la mail diffamatoria è stata inviata utilizzando la rete Fastweb della XY che come specificato dal marito di questa, era senza protezione e perennemente accessibile in quanto il router non veniva mai spento.
È indubbio che chiunque sia stato il reale autore, necessariamente ha dovuto trovarsi nelle immediate vicinanze dell'abitazione della XY, tanto da poter consentirgli di *bucare* la rete wireless della stessa. Notoriamente i router ad utilizzo domestico/non professionale hanno una portata limitata.

Tale libertà di azione, in capo ad una persona in possesso di buone conoscenze informatiche e della struttura di Internet, consentono a questa di poter addebitare la *paternità* di una e-mail (nella presente ipotesi diffamatoria) ad una persona ignara, esponendola così a conseguenze anche di carattere penale.

Nel caso in argomento, l'aver indicato artatamente un orario di invio diverso da quello reale (**07:12:45 +0200** invece di **17:45:56 +0200**), denota volontà da parte del reale autore di collocare l'invio del messaggio in un orario di comodo per lui, al fine di poterlo utilizzare come alibi, ovvero poter mascherare la propria reale collocazione temporale in luogo diverso da quello effettivo.

Nel prosieguo della attività di indagine delegata, considerando che la parte lesa già in allegato alla denuncia aveva prodotto copia cartacea della mail diffamatoria, da cui, però, non si rilevano i destinatari inseriti nel campo CCN (copia conforme nascosta), seppur anch'essi chiaramente e nominativamente indicati nel corpo della denuncia, questa PG, quindi, ha ritenuto opportuno convocare presso questi uffici due soggetti a campione tra quelli indicati. In data [….] sono stati convocati, perciò, i professori [….]**,** docenti c/o l'università […].
I predetti, sentiti a sommarie informazioni, hanno confermato la ricezione della e-mail diffamatoria in argomento [all.ti 13 e 14].
La medesima operazione di acquisizione della e-mail, già espletata con la parte lesa, è stata effettuata sugli account delle caselle di posta elettronica dei due professori. Detta operazione, ha consentito di acquisire copia cartacea della medesima e-mail utilizzata per l'avvenuta diffamazione [all.ti 15 e 16].

L'ulteriore attività è stata indirizzata, quindi, anche nei confronti della persona del fidanzato della parte lesa, già identificato in **BB**. Questo in virtù del legame sentimentale che univa i predetti ma anche perché, sempre la parte lesa, aveva indicato chiaramente in denuncia quale potenziale testimone il proprio fidanzato, peraltro anch'esso segnalato come destinatario della e-mail diffamatoria.
[…] veniva sentito il **BB** a sommarie informazioni, nel corso delle quali lo stesso ha dichiarato quanto sinteticamente riportato di seguito [all.to 17]:
– esplica attività lavorativa presso l'università […], ove si occupa del coordinamento dell'attività dell'assistenza tecnica informatica (hardware e software) all'interno dell'ateneo;

– ha, in questa sede, confermato la conoscenza con la parte lesa, con la quale ha intrattenuto una relazione sentimentale dal 2006 al 2008. Ha precisato di aver convissuto con la p. l. nell'abitazione di quest'ultima, fino all'agosto del 2008;
– ha confermato di aver conosciuto il **CC** in occasione di una vacanza in Mar Rosso fatta nel gennaio del 2007, insieme alla parte lesa;
– tre o quattro mesi dopo, la parte lesa gli avrebbe parlato dei rapporti di collaborazione professionale nati con il **CC**, in particolare che l'impresa […] di quest'ultimo veniva gestita sotto il profilo organizzativo e amministrativo, dalla stessa **AA**;
– nel mese di giugno 2007, la **AA** organizzò una gita […]. Nella circostanza la parte lesa, secondo quanto riferito dal **BB**, aveva organizzato tale escursione senza lo stesso, giustificando ciò con il fatto che vi avrebbero partecipato anche docenti dell'ateneo, a suo dire ignari della relazione esistente tra i due. Occasionalmente il **BB** scoprì che, in effetti, la gita venne fatta […] e non […], questo perché trovò un depliant […]. Il giorno della gita il **BB** contattava più volta la parte lesa sul cellulare ma quest'ultima gli avrebbe sempre risposto in maniera molto evasiva. In sostanza, insospettitosi, si recò presso [….] unitamente a propri amici. Dopo aver atteso tutta la giornata nel parcheggio, a tarda sera vide arrivare la **AA**, con […] lo stesso **CC**, un amico della AA […]**.** Nella circostanza il **BB**, evidentemente sorpreso, tentò di avere spiegazioni dalla parte lesa, ma quest'ultima replicò testualmente: "*cosa ci fa qui, io e te è da mesi che non ci vediamo*". Conseguentemente, la relazione per un certo periodo di tempo si interruppe;
– ha confermato di avere anch'esso ricevuto la e-mail diffamatoria, e proprio questa fu la causa di definitiva cessazione della convivenza con la parte lesa;
– ha dichiarato di non conoscere né XY né YX;
– ha soggiunto di aver avuto la disponibilità diretta all'utilizzo del PC portatile della **AA**, in virtù della loro convivenza.

Atteso che la parte lesa, in denuncia, ha anche segnalato l'avvenuto accesso abusivo alle proprie caselle di posta elettronica, già sopra specificate, avvenuto nell'arco del primo semestre del 2008 […] è stata richiesta l'emissione di opportuni provvedimenti per l'acquisizione dei files di log.
[…] veniva quindi trasmesso per l'esecuzione, alla Microsoft, il provvedimento relativo alla casella di posta elettronica *aa@hotmail.com*, con arco temporale 1/1 – 30/6/2008 [all.to 18].
[...] la Microsoft fornisce i dati richiesti; dati che, per confermando la titolarità della casella di posta in capo alla **AA** e che la stessa è stata attivata in data […] 2001, di fatto non sono utilizzabili ai fini investigativi, perché tutti riferibili a collegamenti avvenuti nel corso dell'anno corrente, e non al periodo di interesse [all.to 19].
Analogamente […] veniva trasmesso, per l'esecuzione, il provvedimento alla Tiscali, presso cui era accesa la casella di posta elettronica *aa@tiscali.it* [all.to 20].
Solo in data […], si è ricevuta la risposta di Tiscali, dopo averla sollecitata in data […] e […] [all.to 21].
Il provider fornisce i dati richiesti e riferiti al periodo di interesse però, purtroppo, comunica di non mantenere files di log relativi ai cambi password, come comunicatoci a seguiti di ulteriore nostra richiesta di chiarimenti [all.to 22].

[…] A seguito di sua delega […] gli scriventi hanno provveduto ad interrogare, con le garanzie della difesa, l'indagato CC, assistito dal proprio legale di fiducia […]
Il predetto, in sede di interrogatorio, pur confermando le circostanze in cui ha conosciuto la AA, ha, di fatto, rigettato in toto le accuse rivoltegli specificando che, in particolare, i fatti indicati nella querela non sono riferibili a episodi realmente avvenuti [all.to 1].

Considerato, quindi, quanto fin qui emerso, in particolar modo le risultanze già riferite con annotazione […], nonché in relazione a quanto qui dichiarato dall'indagato, circa le proprie elementari conoscenze in ambito informatico e, di contro, le qualificate cognizioni nello stesso ambito del fidanzato della parte lesa, BB unici veri *attori* della vicenda oggetto del presente procedimento – pur ovviamente nelle rispettive e differenti posizioni, si reputa opportuno, salvo diverso avviso di codesta A.G., richiedere

l'**emissione di un decreto di acquisizione dei tabulati del traffico telefonico (compreso le relative celle di localizzazione) delle utenze risultate intestate o nella disponibilità dei predetti, per i giorni dal 1° agosto 2008 al 10 agosto 2008 compreso**.
Questo perché l'attività investigativa fin qui svolta non ha, purtroppo, consentito di individuare inequivocabilmente la persona fisica che ha materialmente inviato la e-mail diffamatoria. Pertanto, l'eventuale accoglimento della ipotesi investigativa (emissione del decreto richiesto) consentirebbe agli scriventi di rilevare eventuali tracce di presenza nell'area e nei giorni di interesse (via Carlo Farini di Milano, adiacenze abitazione dei signori XY/YX), dell'autore dei fatti reato ora in contestazione al **CC**.

Si specifica che, da accertamenti svolti presso i vari gestori di telefonia mobile è risultato quanto di seguito:
4. **CC** ha in uso o disponibilità i seguenti telefoni cellulari: […]
5. **BB** ha in uso o disponibilità i seguenti telefoni cellulari: […]

Conseguentemente, dopo l'avvenuta rituale notifica dei provvedimenti in argomento, i gestori hanno qui comunicato quanto segue:
6. **CC:** […] gestore TIM – 7/8/2008 ora 09,17 fino alle ore 23,35, utenza rilevata da una cella con copertura "CGI/Connection IP/NAZ" GRC (Grecia); […]
– BB: […] gestore VODAFONE – 7/8/2008 ore 17,36, utenza rilevata dalla cella identificata come 15001-6381-MI-Milano-via Farini 30-UMTS, Sett.1.

Per chiarezza di esposizione, si richiama nuovamente quanto già esposto nella precedente annotazione […], ovvero:

"... Da una ennesima ed ancor più approfondita lettura dell'header del messaggio diffamatorio si nota una considerevole differenza di orario tra quello posto dal client "Microsoft Outlook 6" (Thu, 7 aug 2008 07:12:45 +0200) e quello inserito dal server di Fastweb (Thu, 7 aug 2008 17:45:56 +0200). Considerato che l'orario reale non può che essere quello inserito dai server interessati alla lavorazione dell'e-mail, ritenendo che sia impossibile, se non a causa di problemi tecnici, che trascorrano circa 10 ore dall'invio del client alla ricezione del primo server, sono stati richiesti chiarimenti, anche in questo caso, a Fastweb. In data 8 ottobre 2009, a tale proposito, si otteneva la seguente risposta [all.to 10] – ***vi precisiamo che il gruppo data orario del corpo del messaggio è un dato configurabile dal client dell'utente; inoltre, in data 7 agosto 2008 non risultano esserci stati problemi o sospensioni nell'erogazione del servizio di invio/ricezione mail sui mail-server Fastweb.****".*

Ciò considerato, quindi, nelle ventiquattro ore del giorno 7 agosto 2008, come sopra evidenziato e risultante dal tabulato fornito dal gestore, l'utenza mobile nr. […] intestata ed in uso all'indagato, **CC**, non risulta presente nell'area di copertura di celle che insistono sul territorio nazionale bensì in quello della Grecia.

Di contro, nel medesimo arco temporale, riferito sempre al giorno 7 agosto 2008, l'utenza mobile nr. […] intestata ed in uso al **BB** risulta, invece, presente nell'area di copertura di celle che insistono sul territorio nazionale.
In particolare, considerato che poco prima dell'invio (7 agosto 2008 ore 17,36) della mail diffamatoria (7 agosto 2008 ore 17,45), la cella così indicata "15001-6381-MI-Milano-via Farini 30-UMTS, Sett.1", processando una chiamata proveniente da un numero di rete fissa e diretta all'utenza mobile del **BB**, ne ha così automaticamente rilevato la presenza nella propria area di copertura.
Detto particolare, tecnico consente di dimostrare la presenza di **BB** nelle immediate vicinanze della abitazione di XY (Milano via Carlo Farini nr. 3x) e, quindi, l'utilizzo della rete wireless di quest'ultima per l'invio della mail diffamatoria.

A seguito di quanto riferito con l'ultima annotazione cui si fa seguito, al fine di avere ulteriori chiarimenti, si è interessata la società Vodafone per farsi specificare l'area di copertura della cella così contraddistinta: **15001-6381-MI-Milano-via Farini 30-UMTS,Sett.1**.
Nella circostanza veniva anche richiesta quale fosse, invece, la cella di copertura sulla via […] di Milano, abitazione della parte lesa **AA**, condivisa durante la loro relazione sentimentale, con il noto **BB**.
La risposta della Vodafone, nell'ordine, è stata:
7. *per quanto concerne l'acquisizione della mappa di copertura della cella UMTS di via Farini nr. 30, settore 1, vi comunichiamo che non è possibile riprodurre graficamente tale informazione per il seguente motivo. Il livello di segnale UMTS dipende da molteplici fattori tra cui la potenza al connettore d'antenna dei nostri impianti, il numero di utenti contemporaneamente collegati e la tipologia di servizi da essi richiesti. Una mappa di copertura UMTS, intesa come insieme dei punti del territorio in cui gli utenti possono accedere alla rete UMTS per mezzo di una determinata cella, potrà essere solo una fotografia "istantanea" di una determinata combinazione di questi parametri, variabile sensibilmente in funzione del tempo. ...* [all.to 1];
8. *le celle che coprivano […] alla data del 7/8/2008 erano: […]* [all.to 2].

In relazione alle risultanze di carattere tecnico appena sopra richiamate, gli scriventi hanno ritenuto utile – per il tramite del sito Google maps – verificare le distanze (a piedi) intercorrenti tra i tre siti di interesse investigativo.
Pertanto, è emerso quanto segue:
– la distanza tra il civico 30 (esatta ubicazione della cella UMTS che ha rilevato la presenza dell'utenza telefonica mobile nr. […], intestata ed in uso a **SG**) ed il civico 3x (abitazione di XY presso cui era, all'epoca dei fatti, installata la rete wireless utilizzata ad insaputa e contro la volontà della titolare per l'invio della mail diffamatoria) di questa via Carlo Farini è risultata essere di soli 0,1 Km [all.to 3];
– la distanza tra il civico 3x di questa via Carlo Farini e il civico […] (abitazione della parte lesa AA) è risultata essere di […] Km [all.to 4];
– la distanza tra il civico 30 di questa via Carlo Farini ed il civico […] è risultata essere di […] Km [all.to 5].

Per completezza e ad ogni buon fine, si è provveduto anche a trasferire su supporto ottico non riscrivibile i file relativi alle e-mail acquisite con il consenso della parte lesa nelle date […], già trasmesse in formato cartaceo con precedente annotazione. Si fa presente che il CD-R contiene nr. 3 files: scuseù.txt; Re scuse.eml; HashFile.xls (hash value dei due precedenti files). Supporto contraddistinto dal numero di questo procedimento penale e firme degli scriventi.

[…] si partecipa che il numero telefonico di rete fissa che ha chiamato l'utenza telefonica mobile del **BB** […] alle ore 17,36 del giorno 7 agosto 2008 (chiamata riferibile all'aggancio del predetto cellulare dalla cella UMTS ubicata in questa via Carlo Farini nr. 30) risulta essere **02.xxxxxxx**.
L'accertamento svolto ha permesso di stabilire che lo stesso risulta intestato a: […] via dove risulta ubicato l'impianto telefonico [all.to 1].

Sentito a sommarie informazioni dal pubblico ministero, il BB confermava l'utilizzo esclusivo del cellulare in esame, precisando che il numero fisso che risulta chiamante alle ore 17,36 del giorno 7 agosto 2008 (chiamata riferibile all'aggancio alla cella UMTS ubicata in via Carlo Farini nr. 30) era del suo commercialista.

Il verbale a questo punto veniva interrotto, pur negando lo stesso gli addebiti.

I computer in uso all'indagato venivano sequestrati, con perquisizione domiciliare immediatamente successiva alla sospensione del verbale (atto al quale ha assistito il difensore, *medio tempore* nominato dal BB).

All'esito dell'indagine, veniva esercitata l'azione penale ed iniziava un faticoso processo indiziario presso il tribunale di Milano. Si riporta l'imputazione:

A) Delitto p. e p. **artt. 61 nn. 2 e 11, 81, 615-*ter*, 617 comma 1 c.p**. perché, dopo aver abusivamente acceduto alla casella di posta elettronica *aa@tiscali.it* e *aa@hotmail.com* (sistema informatico protetto da misure di sicurezza), fraudolentemente prendeva cognizione delle comunicazioni *e-mail* intercorse tra la sua fidanzata AA e CC e a lui non dirette, al fine di commettere il reato di cui al capo B) e con abuso delle relazioni di coabitazione.

In Milano, in epoca prossima ed anteriore al 7 agosto 2008

B) Delitto p. e p. **artt. 81, 494, 595 comma 1 e 3 c.p.** perché, al fine di arrecare ad altri un danno, si attribuiva falsamente l'identità di CC (che, al momento dei fatti, si trovava all'estero e precisamente in Grecia) e, facendo apparire come mittente l'indirizzo *cc@fastwebnet.it* ed un fittizio orario di invio nelle ore 7.12*,* transitando nei pressi del civico 3x di via Farini (come attestato dai tabulati telefonici, avendo lo stesso ricevuto sul proprio cellulare 348.xxxxxx una chiamata alle ore 17.36 proveniente dal numero 02.xxxxx e registrata nella cella VODAFONE di via Farini 30) utilizzava la rete wireless non protetta intestata a M.D. per inviare – con IP 1.18.54.161, a lui non riconducibile – una e-mail nella quale venivano anche allegati alcuni precedenti messaggi di posta elettronica a contenuto anche sessuale tra la AA ed il CC accompagnati dal seguente testo (apparentemente proveniente dal CC ma in realtà redatto dal BB):

"*... OMISSIS insistevi per vederci nell'ora di pausa perché dicevi che ti piacevano ed eccitano OMISSIS* […] *magari riuscirai a giustificare una casa da 600 mila Euro e una Mercedes da 60 mila. Ma come fa una OMISSIS a permettersi un guardaroba e accessori tutti firmati?* […] *a Dicembre hai commesso la cosa più spregevole che potevi fare mandandomi quei gorilla a casa mia per riempirmi di botte e rubarmi il Rolex che mi avevi dato mentre c'era anche mio figlio che ancora adesso è terrorizzato"*

e-mail che veniva inviata ad indirizzi di posta elettronica (tutti presenti nei contatti del computer della AA) di più persone e precisamente a numerosi colleghi di lavoro presso lo XY e conoscenti della AA, che ne avevano così cognizione con conseguente offesa dell'onore e della reputazione della persona offesa.

In Milano, 7 agosto 2008, ore 17.45

C) Delitto p. e p. **artt. 61 n. 11, 81, 646 c.p.** perché, in qualità di dipendente della XY e precisamente quale coordinatore dell'attività di assistenza tecnico informatica, per procurarsi un ingiusto profitto e con abuso delle relazioni di prestazione d'opera, si appropriava dei seguenti beni mobili in suo possesso:

- HD abbinato al computer portatile marca IBM modello THINPAD (numero inventario *OMISSIS*) di proprietà dello XY e non ritrovato dalla PG durante la perquisizione avvenuta in data 12 aprile 2010;
- computer portatile DELL modello PP12F (numero inventario *OMISSIS*) di proprietà dello XY e concesso al CC per il mero utilizzo interno *OMISSIS*, ma ritrovato dalla PG presso il suo domicilio durante la perquisizione avvenuta in data 12 aprile 2010

In Milano, in epoca prossima ed anteriore al 12 aprile 2010

Il dibattimento si concludeva con la condanna alla pena di due anni mesi sei di reclusione ed euro 200,00 di multa[5]. La Corte di Appello di Milano assolveva l'imputato[6] per la sola prima parte del capo C, rideterminando altresì la pena finale in complessivi mesi 10 di reclusione ed euro 100 di multa. La Suprema Corte coglieva l'occasione per precisare l'ambito di diversa operatività tra l'art. 616 e l'art. 617 c.p.[7],

[5] Tribunale di Milano, Sez. 11 penale in funzione monocratica, n. 11808/13 – est. Gurgo di Castelmenardo.

[6] Attesa l'assenza dell'elemento psicologico stante altresì l'assenza di una specifica richiesta di restituzione da parte del proprietario.

[7] "Pur nell'ambito di una non nitida sistematica quale è quella che caratterizza le incriminazioni poste a tutela della inviolabilità delle comunicazioni, deve ritenersi che la possibile interferenza tra le fattispecie punite dagli artt. 616 e 617 c.p. (determinata dalla comune previsione della condotta di colui che prende cognizione della corrispondenza o delle comunicazioni altrui) sia solo apparente. In realtà le stesse hanno ambiti operativi ben definiti dalla diversa configurazione dell'oggetto materiale della condotta,

dichiarando altresì prescritto il reato di diffamazione e rinviando alla Corte di Appello di Milano gli atti per la rideterminazione finale della pena, di seguito fissata in mesi 8 di reclusione e 100 euro di multa[8].

Ovviamente quello che qui rileva non è la vicenda personale[9] dei tre (sia pure drammatica per la persona offesa) ma dare conto di un caso che – nella sua apparente semplicità – è sintomatico di un utilizzo sempre più frequente di rete bucate al fine della commissione di reati informatici.

Inoltre appare altresì evidente quanto già ricordato in un altro caso pratico, ovvero che anche il più ingegnoso disegno criminoso possa spesso scontrarsi con quell'imprevedibile "granello di sabbia che fa inceppare il meccanismo"[10], anche se in ipotesi congegnato come tra i più sofisticati a livello tecnico.

---

anche indipendentemente dalle specifiche connotazioni modali che la caratterizzano nell'art. 617 e che invece non sono previste nell'art. 616. Orbene, non è dubitabile che sul piano concettuale la "corrispondenza" costituisca null'altro che una *species* del *genus* "comunicazione", ma è altrettanto indubbio che nell'ambito dell'art. 617 c.p. quest'ultimo termine non identifichi il *genus* nella sua astratta omnicomprensività, ma assuma un significato maggiormente specializzato, riferibile al profilo "dinamico" della comunicazione umana e cioè alla trasmissione in atto del pensiero, come suggeriscono anche l'ulteriore termine dispiegato per definire l'oggetto materiale del reato ("conversazione") e le condotte alternative a quella di fraudolenta cognizione idonee ad integrare il fatto tipico (interrompere ed impedire). Allo stesso modo, nell'art. 616 c.p., l'evocazione del concetto di "corrispondenza" risulta invece funzionale ad individuare la comunicazione umana nel suo profilo "statico" e cioè il pensiero già comunicato o da comunicare fissato su supporto fisico o altrimenti rappresentato in forma materiale ed anche in questo caso il contenuto delle altre condotte tipizzate alternativamente a quella di illecita cognizione (sottrarre, distrarre, sopprimere e distruggere) conforta le conclusioni rassegnate. In tal senso deve allora concludersi che la condotta contestata all'imputato – e cioè aver preso cognizione del contenuto della corrispondenza telematica intercorsa tra la C. ed il B. conservata nell'archivio di posta elettronica della prima – proprio in virtù della configurazione del suo oggetto materiale, deve essere ricondotta all'alveo dell'art. 616 commi 1 e 4 c.p. e non già, come ritenuto dai giudici di merito, a quello degli artt. 617 comma 1 (anche tenendo conto della sua integrazione ad opera dell'art. 623-bis c.p.)": così Cass., Sez. V, 15 marzo 2017, n. 12603, in *Guida Dir*., 2017, 18, 78 ss. con nota di D. MINOTTI, *I contenuti già visti non si considerano più "corrispondenza".*

[8] Corte di Appello di Milano, sentenza n. 985/2018 (passata in giudicato).

[9] Deve essere considerato il fatto che sono in aumento denunce (attinenti a reati informatici) che si inseriscono in vicende di relazioni sentimentali "naufragate".

[10] L'immagine è mutuata da G. GUASTELLA, *Le nuove truffe. Via sms,* in *www.corriere.it,* 24 febbraio 2008.

CASO PRATICO N. 11

Il 'blog anti-premier' e il paradosso della privacy

a cura di F. CAJANI

Cap. 7 – L'ACQUISIZIONE DEI DATI DEL TRAFFICO
PARTE II: TABULATI TELEFONICI E LOG FILES
Par. 1: Tabulati telefonici e log files come irrinunciabili spunti investigativi ed importanti fonti di prova

L'importanza, non solo per la materia dei reati informatici ma più in generale degli accertamenti tecnologici nelle investigazioni penali, dell'acquisizione dei log files è emersa in tutta la sua complessità in un famoso caso che anni addietro ha interessato la procura della Repubblica presso il tribunale di Milano.

Con provvedimento datato 5 marzo 2009, e dopo quasi un anno di indagini, veniva richiesta l'archiviazione non essendo stato possibile identificare, con relativa certezza, l'autore di due messaggi con i quali veniva proposta, su uno dei più famosi blog dell'epoca, l'uccisione dell'allora Presidente del Consiglio Silvio Berlusconi:

PREMESSO CHE

In data 9 giugno 2008, sulla rete Internet ed in particolare sul blog di Beppe GRILLO, all'indirizzo http://www.beppegrillo.it/2008/06/passaparola_lun_1_2#page_7 venivano postati due commenti, inviati rispettivamente alle ore 18:43 ed alle ore 15:50 ed aventi lo stesso testo, in cui l'autore propone l'uccisione del Presidente del Consiglio Silvio BERLUSCONI.
*Entrambi i messaggi riportavano come mittente tale "**XY**".*
Della presenza di predetti messaggi, in data 10 giugno 2008, veniva data segnalazione al Procuratore della Repubblica presso il Tribunale di Milano, il quale delegava per gli adempimenti del caso il pool reati informatici della Procura.
I commenti sono stati visibili sulla pagina web fino al 20 giugno 2006, alle ore 15:00 circa, come di seguito verrà chiarito […]

A seguito dei primi accertamenti effettuati, veniva richiesta al GIP l'emissione di un decreto di sequestro preventivo.
Al provvedimento del GIP, datato 17 giugno 2008, veniva data esecuzione ad opera della Squadra reati informatici della Procura, delegata al proseguo delle indagini, tutte compendiate nella annotazione di PG del 28.2.2009[1] che qui si richiama per facilità di lettura (con i relativi allegati al fascicolo processuale):

In data 20 giugno 2008, a seguito dell'emissione del predetto Decreto di sequestro preventivo, ed al fine di notificare il provvedimento, si effettuava accertamento al *WHOIS*, individuando come intestatario del dominio la società […] che, con mail inviata alle ore 15:06, comunicava di aver tempestivamente provveduto alla cancellazione dalla pagina dei commenti oggetto del procedimento penale.
Si dà atto che lo stesso giorno alle ore 15:10 lo scrivente, collegatosi all'indirizzo *http://www.beppegrillo.it/2008/06/passaparola_lun_1_2.html#page_7*, accertava che i due commenti non erano più visibili, come si evince dal Verbale delle operazioni compiute redatto dallo scrivente in pari data (**ALLEGATO 3**), che contiene anche, in allegato, tutta la documentazione riguardante questa parte di attività svolta.

[1] Annotazione a firma dell'UPG Giacinto Bigaroli e dell'APG Paolo De Feo, squadra reati informatici della procura di Milano. Le note dalla 2 fino alla 26, dalla 30 alla 40, nonché dalla 41 alla 44 sono parte integrante dei rispettivi provvedimenti del pubblico ministero Francesco Cajani.

Contemporaneamente è stata svolta attività di P.G. finalizzata all'individuazione del soggetto che ha inviato i commenti oggetto del procedimento.

Preliminarmente è opportuno far presente che il *blog* in menzione permette l'invio di un commento all'argomento in trattazione mediante la compilazione del *form* (modulo) che si trova al termine della pagina *web* (**ALLEGATO 4**). Come si evince, prima di inserire ed inviare il commento il lettore è invitato a leggere le avvertenze che, per comodità di lettura vengono di seguito riportate:

> **Inserisci il tuo commento**
> *Il Blog di Beppe Grillo è uno spazio aperto a vostra disposizione, è creato per confrontarsi direttamente. L'immediatezza della pubblicazione dei vostri commenti non permette filtri preventivi. L'utilità del Blog dipende dalla vostra collaborazione per questo motivo voi siete i reali ed unici responsabili del contenuto e delle sue sorti.*
>
> **Avvertenze** da leggere prima di intervenire sul blog di Beppe Grillo
>
> **Non sono consentiti:**
> – messaggi **non inerenti al post**
> – messaggi **privi di indirizzo email**
> – messaggi **anonimi (cioè senza nome e cognome)**
> – messaggi **pubblicitari**
> – messaggi con **linguaggio offensivo**
> – messaggi che **contengono turpiloquio**
> – messaggi con **contenuto razzista o sessista**
> – messaggi il cui **contenuto costituisce una violazione delle leggi italiane** (istigazione a delinquere o alla violenza, diffamazione, ecc.)
>
> Comunque il proprietario del blog potrà in qualsiasi momento, a suo insindacabile giudizio, cancellare i messaggi.
> In ogni caso il proprietario del blog non potrà essere ritenuto responsabile per eventuali messaggi lesivi di diritti di terzi.

I lettori che inviano eventuali commenti possono essere "certificati" oppure non esserlo; per la "certificazione" è necessario preliminarmente compilare il *form* (**ALLEGATO 5**) che consente l'autenticazione con *password*; l'invio di un commento da parte di un lettore certificato è indicato con un'icona accanto al nome dello stesso, come nell'esempio in ***Figura 3***.

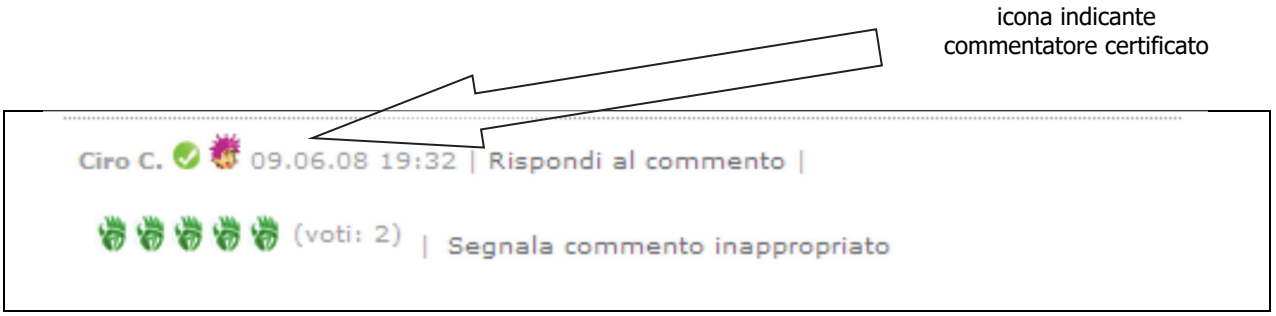


Figura 3
– Commentatore certificato –

Il lettore non certificato, come si legge nell'Informativa Privacy (si rimanda all'**ALLEGATO 4**), per poter postare un commento oltre all'*email*, deve inserire il nome e cognome; è prevista la possibilità di memorizzare o meno i dati.
Nome e cognome vengono pubblicati e, quindi, *diffusi* sul Web unitamente al commento postato dall'utente, l'indirizzo e-mail viene utilizzato esclusivamente per l'invio delle *news* del sito. Le opinioni ed i commenti postati dagli utenti e le informazioni e dati in esso contenuti non saranno destinati ad altro scopo che alla loro pubblicazione sul *Blog*.

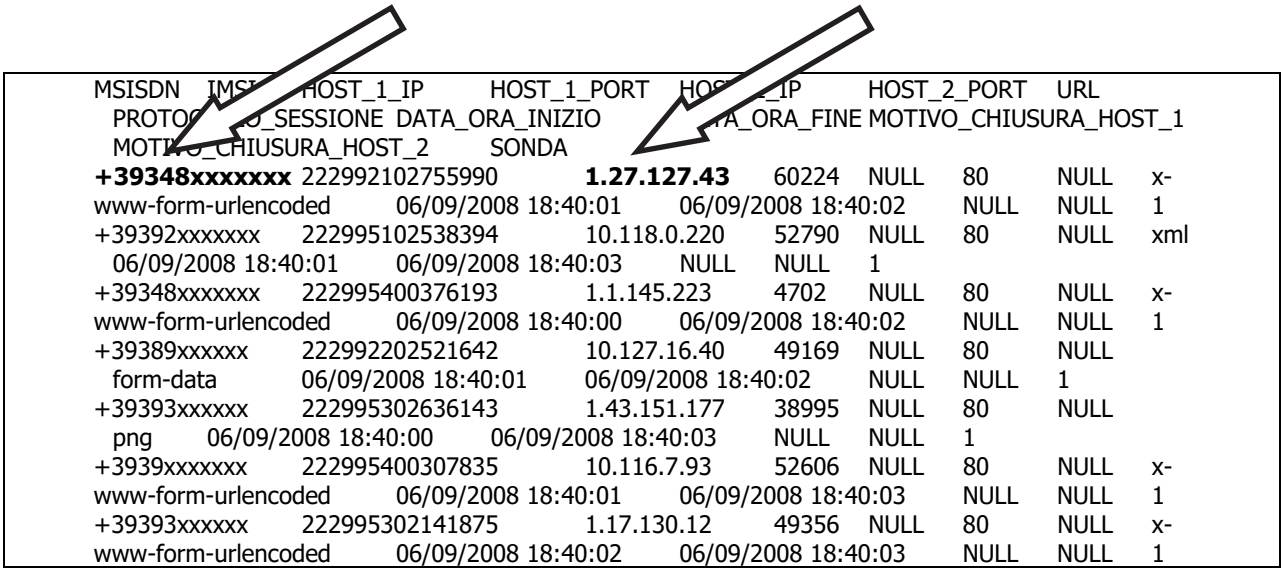
I due commenti oggetto degli accertamenti riportano come nome e cognome del soggetto che ha inviato gli stessi, in tale "**XY**" e non riportano l'icona che contraddistingue i commentatori certificati.
Dalle informazioni ricevute dalla società […] (si rimanda all'**ALLEGATO 3**), peraltro responsabile del trattamento dei dati, si apprende che al momento dell'invio dei messaggi, oggetto del procedimento, il mittente:

• ha inserito come indirizzo mail di riferimento l'account **comicispaventati@hotmail.it**;
• era collegato alla rete con una connessione avente indirizzo IP **62.13.173.176**.

Sulla base di questi ultimi due elementi, al fine di individuare l'utenza connessa negli orari d'invio dei commenti all'indirizzo IP **62.13.173.176**, si procedeva a richiedere al provider assegnatario H3G i dati relativi alle connessioni telematiche, nell'arco di tempo compreso tra le 18:30 e le 19:00, previa notifica del Decreto di acquisizione di dati relativi alle connessioni telematiche (*file di log*) emesso in data 23/06/2008 da codesta A.G. (**ALLEGATO 6**).
Contemporaneamente, al fine di individuare l'utilizzatore dell'indirizzo di posta elettronica **comicispaventati@hotmail.it**, in data 23/06/2008 si procedeva a richiedere alla Microsoft Corporation, per il tramite dell'italiana Microsoft srl […], i dati relativi alla creazione ed agli accessi del predetto indirizzo di posta elettronica **comicispaventati@hotmail.it**, account che preliminarmente si accertava essere esistente (**ALLEGATO 7**).
La società H3G ha dato seguito al provvedimento, inviando via posta con raccomandata A/R un CDRom contenente i dati richiesti ad esclusione degli indirizzi IP di destinazione della connessione telematica, oggetto di richiesta, puntualizzando nella lettera di accompagnamento che "*H3G s.p.a. fa presente che il Garante per la protezione dei dati personali, al fine di tutelare la riservatezza della navigazione in Internet e dell'uso dei motori di ricerca, con provvedimento del 17/01/2008, ha vietato ai gestori di servizi telefonici e telematici, la conservazione in qualsiasi forma del dettaglio e delle informazioni sui siti visitati dagli utenti* (si rimanda all'**ALLEGATO 6**).

È opportuno precisare che l'indirizzo IP fornito, ***nell'arco di tempo richiesto e come di seguito verrà spiegato, risulta essere utilizzato da numerosi utenti***. Infatti la Rete H3G è costruita sull'architettura della NAT[2] (acronimo di *Network Address Translation*). ***In buona sostanza l'indirizzo IP segnalato non è direttamente associabile ad alcun utente H3G, né individua il mittente o il destinatario di alcuna comunicazione di natura telematica***; esso designa piuttosto uno dei punti di acceso fornito dalla Rete H3G, per accedere alla rete pubblica *internet* tramite apparato di telefonia mobile.
Ogni utente H3G, ovvero ogni terminale collegato alla Rete H3G, è univocamente identificato all'interno di essa tramite un indirizzo di rete ad esso associato (indirizzo IP) ed abbinato ad un'utenza mobile (SIM/numero utenza) ed hanno valore locale; assumono, cioè, validità solamente all'interno della loro rete e hanno rilevanza esclusivamente in tale ambito (indirizzi IP privati) (**Figura 4**).

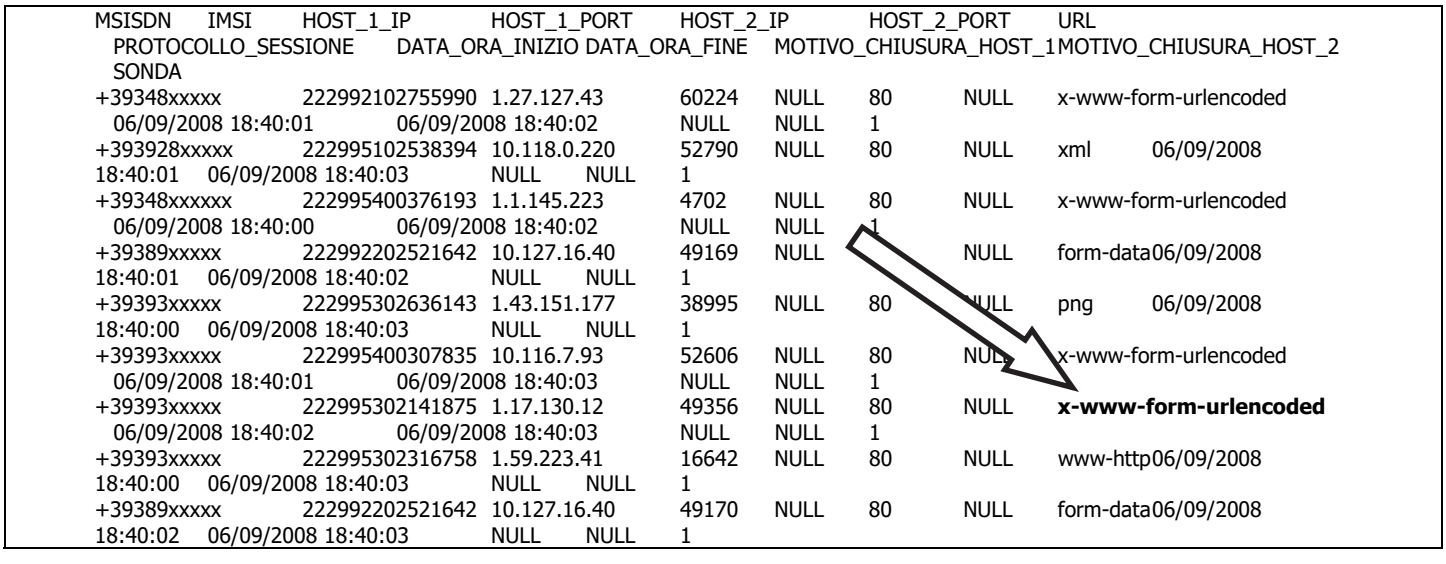
[2] **NAT** (acronimo di Network Address Translation) nel campo delle reti telematiche conosciuto anche come Network Masquerading o Native Address Translation, è una tecnica che consiste nel modificare gli indirizzi IP dei pacchetti in transito su un sistema che agisce da router. Sono molto note anche alcune tipologie specifiche di NAT, come l'IP masquerading e il port forwarding.



MSISDN	IMSI	HOST_1_IP	HOST_1_PORT	HOST_2_IP	HOST_2_PORT	URL
PROTOCOLLO_SESSIONE	DATA_ORA_INIZIO	DATA_ORA_FINE	MOTIVO_CHIUSURA_HOST_1			
MOTIVO_CHIUSURA_HOST_2	SONDA					
+39348xxxxxxx	222992102755990	**1.27.127.43**	60224	NULL	80	NULL
x-www-form-urlencoded	06/09/2008 18:40:01	06/09/2008 18:40:02	NULL	NULL	1	
+39392xxxxxxx	222995102538394	10.118.0.220	52790	NULL	80	NULL
xml	06/09/2008 18:40:01	06/09/2008 18:40:03	NULL	NULL	1	
+39348xxxxxxx	222995400376193	1.1.145.223	4702	NULL	80	NULL
x-www-form-urlencoded	06/09/2008 18:40:00	06/09/2008 18:40:02	NULL	NULL	1	
+39389xxxxxx	222992202521642	10.127.16.40	49169	NULL	80	NULL
form-data	06/09/2008 18:40:01	06/09/2008 18:40:02	NULL	NULL	1	
+39393xxxxxx	222995302636143	1.43.151.177	38995	NULL	80	NULL
png	06/09/2008 18:40:00	06/09/2008 18:40:03	NULL	NULL	1	
+3939xxxxxxx	222995400307835	10.116.7.93	52606	NULL	80	NULL
x-www-form-urlencoded	06/09/2008 18:40:01	06/09/2008 18:40:03	NULL	NULL	1	
+39393xxxxxx	222995302141875	1.17.130.12	49356	NULL	80	NULL
x-www-form-urlencoded	06/09/2008 18:40:02	06/09/2008 18:40:03	NULL	NULL	1	

Figura 4
– Estratto dati forniti da H3G –

Per tale ragione essi non sono conosciuti dalla Rete pubblica *internet*, né direttamente raggiungibili da essa; perché agli utenti H3G sia consentito raggiungere destinazioni pubbliche, tali indirizzi sono dinamicamente trasposti in indirizzi pubblici tramite l'adozione, appunto, di meccanismo NAT (nel caso in menzione 62.13.173.176)
In conseguenza di ciò l'indirizzo di rete del punto d'accesso ad *internet* di volta in volta utilizzato distingue la totalità delle comunicazioni e degli utenti H3G che in un dato momento ne facciano uso.
Per questo meccanismo, nell'arco di tempo contenuto anche in un solo secondo, possono essere connessi decine e decine di utenti (circostanza che di fatto, dall'analisi effettuata, è avvenuta anche in questo caso) e, poiché il Garante per la protezione dei dati personali, come già citato, ha vietato ai gestori di servizi telefonici e telematici, la conservazione in qualsiasi forma del dettaglio e delle informazioni sui siti visitati dagli utenti, nei dati forniti da H3G, non è indicato l'IP di destinazione della navigazione ma un semplice riferimento alla parte iniziale dell'URL *(Acronimo di Uniform Resource Locator è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet, come un documento o un'immagine*) (**Figura 5**).



MSISDN	IMSI	HOST_1_IP	HOST_1_PORT	HOST_2_IP	HOST_2_PORT	URL
PROTOCOLLO_SESSIONE	DATA_ORA_INIZIO	DATA_ORA_FINE	MOTIVO_CHIUSURA_HOST_1	MOTIVO_CHIUSURA_HOST_2		
SONDA						
+39348xxxxx	222992102755990	1.27.127.43	60224	NULL	80	NULL
x-www-form-urlencoded	06/09/2008 18:40:01	06/09/2008 18:40:02	NULL	NULL	1	
+393928xxxxx	222995102538394	10.118.0.220	52790	NULL	80	NULL
xml	06/09/2008 18:40:01	06/09/2008 18:40:03	NULL	NULL	1	
+39348xxxxxx	222995400376193	1.1.145.223	4702	NULL	80	NULL
x-www-form-urlencoded	06/09/2008 18:40:00	06/09/2008 18:40:02	NULL	NULL	1	
+39389xxxxx	222992202521642	10.127.16.40	49169	NULL	80	NULL
form-data	06/09/2008 18:40:01	06/09/2008 18:40:02	NULL	NULL	1	
+39393xxxxx	222995302636143	1.43.151.177	38995	NULL	80	NULL
png	06/09/2008 18:40:00	06/09/2008 18:40:03	NULL	NULL	1	
+39393xxxxx	222995400307835	10.116.7.93	52606	NULL	80	NULL
x-www-form-urlencoded	06/09/2008 18:40:01	06/09/2008 18:40:03	NULL	NULL	1	
+39393xxxxx	222995302141875	1.17.130.12	49356	NULL	80	NULL
x-www-form-urlencoded	06/09/2008 18:40:02	06/09/2008 18:40:03	NULL	NULL	1	
+39393xxxxx	222995302316758	1.59.223.41	16642	NULL	80	NULL
www-http	06/09/2008 18:40:00	06/09/2008 18:40:03	NULL	NULL	1	
+39389xxxxx	222992202521642	10.127.16.40	49170	NULL	80	NULL
form-data	06/09/2008 18:40:02	06/09/2008 18:40:03	NULL	NULL	1	

Figura 5
– Estratto dati forniti da H3G –

Risulta quindi assolutamente impossibile determinare con quale utenza mobile sia stata fatta la connessione telematica utilizzata per l'invio dei commenti oggetto del procedimento penale.

In merito agli esiti degli accertamenti richiesti alla Microsoft Corporation, tramite la Microsoft srl, relativi agli accessi all'indirizzo di posta elettronica **comicispaventati@hotmail.it** (si rimanda all'**ALLEGATO 7**) è opportuno precisare che:

- In data 26/06/2008, la società Microsoft rispondeva in posta elettronica che: "*… l'account risulta non essere più attivo e quindi non risultano più i dati riferiti agli accessi effettuati dal suddetto account ne tantomeno i dati di registrazione. …*".
- Nella stessa risposta Microsoft precisava inoltre che: "*… il database di Microsoft Corporation conserva i dati per un massimo di 60 giorni (cd. **data retention** – ndr), dopo di che vengono cancellati; inoltre se l'account hotmail non viene utilizzato entro 90 giorni questo viene automaticamente disattivato.*"

Poiché dagli accertamenti tecnici effettuati dagli scriventi in data 20/06/2008 è emerso che, contrariamente a quanto comunicatoci precedentemente dalla società Microsoft, l'indirizzo di posta elettronica **comicispaventati@hotmail.it** era ancora attivo, il giorno 24/07/2008, presso l'ufficio del P.M. […], veniva sentita a sommarie informazioni […] la quale riferiva […] che: "*come noto infatti tutti i dati relativi a caselle di posta elettronica dei domini hotmail.com e hotmail.it si trovano negli Stati Uniti sui server dello stato di Washington. Microsoft risponde alle richieste e le stesse sono successivamente inoltrate alle autorità richiedenti, avvalendoci di stagisti dell'ufficio legale, tra i quali, come emerge da alcuni vostri atti, […] che attualmente è l'unica stagista presente. Preciso altresì che a Microsoft s.r.l. arriva l'estrapolazione del dato richiesto su un apposito file excell che poi viene rigirato con una mail di accompagnamento o con un fax di trasmissione. Nel file excell non viene indicato chi materialmente abbia effettuato l'estrapolazione anche se a Microsoft s.r.l. il file arriva tramite una mail aziendale di un collega americano dell'ufficio Microsoft International criminal compliance. Questi ultimi dati tuttavia non vengono inoltrati all'autorità giudiziaria italiana richiedete perche come già precisato il nostro ufficio si limita a trasmettere il file con una mail/faxdi accompagnamento proveniente da Microsoft s.r.l.".*
Nel corso delle sommarie informazioni il P.M., in relazione alle precisazioni indicate nella risposta del 26/06/2008, rappresentava
- la necessità di verificare le ragioni, in fatto e in diritto, che hanno determinato la *policy* di Microsoft Corp. relativa alla conservazione dei dati per un massimo di 60 gg;
- la necessità di verificare quale fosse la policy di Microsoft s.r.l. in materia di conservazione dati attinenti il traffico telematico sulle caselle *hotmail.it, hotmail.com, msn.com, live.it* anche in relazione alla normativa italiana che, attualmente, prevede un obbligo di conservazione peri a 12 mesi.

Nella circostanza […] si riservava di fornire all'A.G. ogni ulteriore indicazione circa l'account **comicispaventati@hotmail.it** e documentazione relativa al periodo di conservazione dei dati da parte di Microsoft.
Il giorno successivo (25/07/2008), a parziale scioglimento delle riserve, […] con una email forniva i dati relativi al predetto indirizzo di posta elettronica precisando che la prima riposta con esito negativo era dovuta ad un banale errore di trascrizione. I dati forniti comprendevano, oltre agli IP di creazione dell'account, anche i Log di connessione, **relativi agli ultimi 60 gg** da tale (successiva) elaborazione.
Sulla base dei dati forniti emergeva che nell'arco di tempo compreso tra l'invio del primo e del secondo commento vi era stato un accesso alla casella di posta elettronica e l'IP di connessione era lo stesso dell'invio dei post (62.13.173.176). Per questo motivo si ritiene plausibile che l'autore degli accessi sia lo stesso dell'invio dei commenti.

Per i motivi sopra esposti, nell'impossibilità di effettuare ulteriori accertamenti sul predetto IP, ci si concentrava sugli accessi effettuati all'indirizzo di posta elettronica **comicispaventati@hotmail.it**, utilizzando connessione fornite da altri I.S.P.
In data 28/07/2008 venivano così richiesti dati relativi alle connessioni telematiche a Telecom Italia s.p.a., che dava riscontro 08/08/2008 (**ALLEGATO 8**) e a Wind s.p.a che dava riscontro in data 06/08/2008 (**ALLEGATO 9**). Da questi ultimi esiti e, in particolare da quelli forniti da Telecom, emergeva che alcune connessioni erano state effettuate utilizzando l'utenza di telefonia fissa [….] intestata a […] (**ALLEGATO 8**). Accertamenti anagrafici permettevano di verificare che questi ha un fratello convivente […]. Una delle connessioni all'indirizzo di posta elettronica **comicispaventati@hotmail.it** risulta essere stata effettuata attraverso l'I.S.P. Telecom utilizzando il nr. […] intestato a […]
Accertamenti effettuati su eventuali utenze mobili intestate [….] (**ALLEGATO 10**), associabili alla connessione telematica utilizzata per l'invio dei post non davano esiti negativi.
Lo stesso [….], in data 26 settembre 2008, veniva assunto a sommarie informazioni testimoniali, nel corso delle quali questi ammetteva di ***avere creato ed avere in uso*** l'account di posta elettronica

comicispaventati@hotmail.it, ma negava di avere inviato i commenti più volte citati; **affermava, inoltre, di avere avuto problemi di accesso all'indirizzo di posta, avanzando l'ipotesi che qualcun altro avesse potuto aver accesso *all'account* di posta elettronica** (**ALLEGATO 11**)"

RILEVATO CHE

1) all'esito della richiamata annotazione, le conclusioni degli operanti di PG sono state così indicate:

Alla luce di quanto finora esposto, **eventuali accertamenti sulla attendibilità delle affermazioni rese da [...] non risultano possibili**, a causa della cancellazione degli IP di destinazione di interesse nonché del breve periodo di *data retention* da parte di Microsoft Corp.

Tali considerazioni sono ampiamente condivise da questo Pubblico Ministero, in quanto il pool reati informatici della Procura di Milano è ben da tempo a conoscenza dello stato attuale delle investigazioni sul cyber crime alla luce degli ostacoli tecnici/normativi che, anche in questa indagine, "puntualmente" si sono verificati.

Infatti:

a) ove fossero stati conservati gli IP di destinazione, sarebbe stato agevole identificare compiutamente sulla rete NAT l'effettivo indirizzo IP[3] *utilizzato per inserire, come indirizzo e-mail di riferimento,*

[3] Infatti, immaginando di dover trovare un riscontro investigativo ad un accesso abusivo (avvenuto in determinato giorno/ora) tramite webmail alla casella di posta elettronica del querelante, i dati a disposizione dell'investigatore sono:

[A] data e ora dell'evento informatico,

[B] indirizzo e-mail del querelante,

[C] IP della pagina web che rende disponibile l'accesso alla casella di posta elettronica, ovvero l'IP della webmail.

Richiesti i log degli accessi all'IP sub [C] al gestore interessato (ricavabile dall'informazione sub [B]), possiamo ottenere la seguente tipologia di dati (si riporta una "ipotesi di scuola"):

Indirizzo IP: 87.2.165.21
Data/ora inizio connessione: 9.6.2007 11:00
Data/ora fine connessione: 9.6.2007 14:30

Data Inizio	Ora Inizio	Data fine	Ora Fine	Login Cliente
09.06.2007	11:00	09.06.2007	12:00	****
09.06.2007	12:00	09.06.2007	12:12	****
09.06.2007	12:12	09.06.2007	14:30	****

L'investigatore dovrà estrapolare il risultato utile per il proseguo delle indagini facendo uso delle informazioni sub [A]: si potrà quindi così risalire ai dati relativi all'utente a cui l'ISP ha dato connessione.

Questo tuttavia si verifica – come ben evidenziato dagli operanti di PG – laddove il gestore richiesto non utilizzi, per far fronte alla limitazione di indirizzi IP supportabile dall'attuale versione del protocollo internet IPv4, un sistema NAT/PAT (Network & Port Address Traslation) tramite il quale – ad un unico IP pubblico – vengono abbinati diversi indirizzi IP d'origine.

Infatti, in questo secondo caso, i log che tale gestore era solito fornire – prima dell'intervento dell'Autorità Garante – erano i seguenti (si riporta anche in questo caso una "ipotesi di scuola"):

Elenco delle comunicazioni iniziate e finite all'interno dell'intervallo di tempo richiesto Ricerca Traffico Storico per IP/Porta Nattato: 213.140.6.***/* Data Inizio: 09/06/2007 11:00:00 Data Fine: 09/06/2007 14:30:00				
IP Sorgente	**IP Destinazione**	**Porta destinazione•**	**Data Inizio**	**Data fine**
1.31.217.**	62.1.240.208	10076	07-04-2007 11:00:00	07-04-2007 11:00:09
1.11.216.**	194.20.158.102	80	07-04-2007 11:00:00	07-04-2007 11:00:07
1.8.91. **	62.149.128.152	80	07-04-2007 11:00:00	07-04-2007 11:00:01
1.11.216.**	217.12.4.128	80	07-04-2007 11:00:00	07-04-2007 11:00:00
1.5.215.***	82.57.161.5	4662	07-04-2007 11:00:00	07-04-2007 11:00:46
1.5.96.**	213.146.220.118	20372	07-04-2007 11:00:00	07-04-2007 11:00:43

l'account ***comicispaventati@hotmail.it*** *(e quindi l'indirizzo IP utilizzato per l'inserimento del messaggio stesso)*

b) ove Microsoft avesse conservato i files di log relativi a tale casella per il periodo di tempo imposto dalla normativa italiana (12 mesi) o comunque comunitaria (almeno 6 mesi come termine minimo) in materia di data retention, gli operanti di PG sarebbero stati messi nella condizione di estendere ulteriormente le verifiche tecniche, per accertare se ***effettivamente potesse essere riconducibile al […] non solo l'attività di creazione di tale e-mail ma anche il suo utilizzo continuativo fino all'attività di inserimento del messaggio sul blog****.*

Tutto questo, invece, allo stato non risulta praticabile per le ragioni (in diritto più che in fatto) che verranno di seguito indicate.

2) Quanto al problema della ***cancellazione degli IP di destinazione,*** *le complessive vicende*[4] *che hanno portato al definitivo recepimento della Direttiva 2006/24/CE in materia di data retention (di seguito: Direttiva) dimostrano nei fatti come il concetto di privacy venga sempre più spesso contrapposto alle esigenze investigative ed, in particolare, al cd. tracing (primo accertamento tipico – e tecnico – delle indagini sul cybercrime) ovvero a quel "percorso a ritroso" finalizzato a ritrovare l'origine della condotta posta in essere con strumenti informatici.*
Trattasi quindi di una attività di "tracciamento" e non già di "intercettazione" (anche se spesso così viene intesa dai non addetti ai lavori), anche perché i risultati del tracing non sono altro che un indirizzo IP di connessione della macchina dalla quale – verosimilmente[5] *– è partito l'evento informatico costituente ipotesi di reato.*

1.5.215.***	213.254.17.121	80	07-04-2007 11:00:01	07-04-2007 11:00:30
1.5.215.***	220.171.184.136	13076	07-04-2007 11:00:01	07-04-2007 11:00:48
1.22.242.***	212.113.31.48	80	07-04-2007 11:00:01	07-04-2007 11:00:01
1.9.96.**	87.106.28.102	80	07-04-2007 11:00:02	07-04-2007 11:01:17
1.5.215.**	207.159.120.154	80	07-04-2007 11:00:02	07-04-2007 11:00:02
1.23.86.***	84.222.117.126	1060	07-04-2007 11:00:02	07-04-2007 11:00:51
(Tra gli ulteriori dati che identificano il traffico telematico, ci sono quelli relativi alle porte (intese come veri e propri canali attraverso le quali i dati vengono trasferiti) interessate: come noto, la porta 80 è quella che individua la navigazione web.				

L'investigatore, a questo punto, dovrà ricavare l'informazione a lui necessaria facendo utilizzo non solo dei dati sub [A] ma anche – e imprescindibilmente – di quelli sub [C].

In concreto, verificherà lui stesso *aliunde* quale sia l'IP assegnato alla pagina che fornisce l'accesso *webmail* e solo a questo punto riuscirà a portare a termine, con successo, l'analisi dei *files* di log (individuando, tra le tante connessioni all'interno della fascia temporale di riferimento, solo quelle indirizzate verso l'IP di destinazione conosciuto).

Senza il dato sub [C], invece, nella quasi totalità dei casi, non sarà possibile identificare con esattezza quale tra i molteplici IP di origine sia riconducibile – nell'arco temporale sub [A] – alla condotta illecita.

[4] A partire dalla legge 31 luglio 2005, n. 155 (cd. decreto Pisanu) fino alla recente vicenda del cd. decreto "milleproroghe" (fine dicembre 2007) e della sua conversione in legge, preceduta da una lettera al Parlamento ad opera del Garante per la protezione dei dati personali nella quale ribadiva "le proprie preoccupazioni sul periodo di conservazione dei dati di traffico telefonico ed Internet detenuti per finalità di giustizia. Attualmente, dopo il recente decreto "milleproroghe", che ha prolungato i termini fino al 31 dicembre 2008, i tempi di conservazione possono arrivare a 8 anni per i dati di traffico telefonico e a 3 per quelli telematici. L'Autorità ha posto l'esigenza che il bilanciamento degli interessi coinvolti sia conforme alle prescrizioni della direttiva comunitaria in materia (la cosiddetta "direttiva Frattini"), e che la direttiva stessa, la quale prevede tempi di conservazione dei dati di traffico sia telefonico che telematico compresi tra un minimo di sei mesi ed un massimo di due anni, sia tempestivamente recepita": cfr. *www.garanteprivacy.it/garante/doc.jsp?ID=1479338.* Sulla perplessità dei calcoli matematici fatti dal Garante (che presuppongono – ma la realtà potrebbe essere stata ben diversa – che nell'agosto 2005 i gestori avessero già a disposizione dati del traffico fin dal 2001, e che quindi da quel momento li abbiano conservati in virtù del relativo obbligo introdotto *ex lege*) cfr. S. ATERNO, in *Conservazione dei dati informatici e prospettive europee*, atti del Convegno OLAF "Nuove prospettive dell'attività investigativa nella lotta antifrode in Europa", Milano, 24/25 gennaio 2008.

[5] Infatti, abbinato a questo IP possiamo trovare:
I) un computer isolato,

II) un computer in rete (aziendale, wireless),

III) un cd. internet mobile phone (telefoni di ultima generazione, che consentono le connessioni internet) con scheda prepagata, quasi sempre aperta con dati fittizi […].

Con risultati investigativi utili (ove effettivamente venga ritrovata la macchina interessata dalla connessione rintracciata a ritroso) probabilmente favorevoli solo nel caso sub I). […].

*E dunque un **dato esterno alla comunicazione**[6] e, più precisamente, un (semplice) numero di telefono relativo alla richiesta connessione, dal quale – per ovvi motivi – non è possibile automaticamente risalire all'effettivo utilizzatore di quel computer.*
Quindi, visto che non è possibile automaticamente far corrispondere un IP ad un soggetto (autore del reato), non sussisterebbe – per ora – un problema di riservatezza.
Il Gruppo per la tutela dei dati personali – Articolo 29 ha affermato, nel 2002[7], che «gli indirizzi IP attribuiti agli utenti Internet costituiscono dati personali[8] e sono tutelati dalla direttiva 95/46/CEE e 97/66/CEE».
A parere dello scrivente, affermare la natura di dato personale[9] di un indirizzo IP non deve però trarre in inganno l'interprete e portarlo ad affrettate conclusioni.
Infatti, l'IP è un dato che solo se (e in quanto) posto in relazione ad altri dati (ovvero: data e ora di connessione) è in grado di restituirci un risultato potenzialmente lesivo della riservatezza, dal momento che – in una determinata frazione di tempo – l'Internet Service Provider (ISP) attribuisce quel determinato indirizzo IP ad un (solo) utente intestatario del relativo contratto per la connessione ad Internet.
Ma, ancora, nulla sappiamo di questo utente se non il numero di telefono utilizzato dallo stesso e i dati (esterni, come già indicato) relativi alla tipologia della intervenuta connessione.
E pur tuttavia per molti questo sarebbe di per sé solo sufficiente a generare un pericolo per la riservatezza dell'utente stesso.
Si pensi, tra i tanti scritti apparsi qua e là nel corso degli ultimi anni, ad argomentazioni di questo tipo: «L'art. 6 del d.l. 144/05 sancisce l'obbligo di conservazione di tutti i dati di traffico telematico che consentono la tracciabilità degli accessi e dei servizi. In pratica, ciò vuol dire effettuare non solo la conservazione delle informazioni relative all'utilizzo dei servizi, tra gli altri, di posta elettronica, chat, newsgroup, ftp, filesharing; ma anche dei dati I.P. dei servers cui ci si connette – che nelle comunicazioni telefoniche equivarrebbe al numero di telefono chiamato – da cui è facilmente desumibile, ad esempio, l'indirizzo internet delle pagine consultate o almeno delle relative homepage. In tal modo, viene consentita la monitorazione degli accessi internet ed una definizione potenzialmente dettagliata dei gusti, delle abitudini e dell'identità sociale del singolo attraverso una semplice indagine sui siti maggiormente visitati, sulle pubblicità visualizzate o sulla tipologia dei gruppi di discussione cui si è partecipato»[10] .
Nonché, ancor più significativamente, a quanto apparso nell'ultima relazione annuale del Garante per la protezione dei dati personali (che, forse non per caso, mette al secondo posto – tra i "provvedimenti più significativi" dell'Autorità nel 2007 – quelli in materia di "conservazione e sicurezza dei dati di traffico telefonico e telematico": cfr. p. 6): «i gestori devono infatti conservare esclusivamente i dati di traffico telematico funzionali alla fornitura e alla fatturazione del servizio di connessione e non i dati di traffico apparentemente "esterni" alla comunicazione (pagine web visitate o gli indirizzi Ip di destinazione) e che possono peraltro coincidere di fatto con il "contenuto" della comunicazione, consentendo di ricostruire meglio relazioni personali e sociali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute».
Ad una più attenta riflessione, come peraltro i fatti di questo procedimento hanno confermato, si possono meglio comprendere le perplessità messe in evidenza dai primi commentatori[11] fin dall'emanazione del provvedimento generale sulla "Sicurezza dei dati di traffico telefonico e telematico" ad opera del Garante per la protezione dei dati personali[12], in relazione al fatto che la limitazione degli obblighi di

---

[6] Infatti anche un indirizzo IP può considerarsi effettivamente, e non solo "apparentemente", dato esterno (di una comunicazione, informatica). […]

[7] "Parere 2/2002 sull'uso di identificativi esclusivi negli apparecchi terminali di telecomunicazione: l'esempio dell'IPv6" reperibile in Internet all'indirizzo *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_it.pdf.*

[8] "Come specificato dal ventiseiesimo considerando della direttiva 95/46/CE i dati sono qualificati come personali se utilizzando mezzi ragionevoli può essere stabilito un nesso con l'identità dell'interessato (in questo caso, l'utilizzatore di un indirizzo IP) da parte del responsabile del trattamento o da altri. Nel caso degli indirizzi IP, l'ISP è sempre in grado di stabilire un nesso tra l'identità dell'utente e gli indirizzi IP e altri possono essere in grado di fare altrettanto, per esempio facendo ricorso a registri disponibili degli indirizzi IP attribuiti o ad altri dispositivi tecnici esistenti".

[9] *Ex* art. 4 comma 1 lett. b) d.lgs. 196/2003: "qualsiasi informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi informazione, ivi compreso un numero di identificazione personale".

[10] Così M. VIGGIANO, I *dati personali nelle ricerche su Internet*, in *Il Diritto della Informazione e dell'Informatica*, 2007, f. 2, 379.

[11] Cfr. in particolare S. ATERNO, *Intervento sulla mailing list di IISFA* (*International Information Systems Forensics Association*: *www.iisfa.it*) del 7 febbraio 2008.

[12] in G.U. n. 30 del 5 febbraio 2008, nel quale – pur in relazione al combinato disposto degli artt. 17 comma 2 e 132 comma 5

conservazione ai soli IP di origine potrebbe costituire un insormontabile ostacolo negli accertamenti di polizia giudiziaria in materia di cybercrime.
Questo non solo in relazione ai sempre più diffusi sistemi NAT/PAT[13] ma soprattutto ad alcune ipotesi investigative concrete che possono essere qui solo succintamente evocate: senza scomodare casi connessi al cyberterrorismo o alla pedopornografia on line, sarà semplicemente impedita una molteplicità di riscontri informatici ad azioni volutamente poste in essere non solo dall'indagato (nella commissione dei reati) ma anche dalla persona offesa (anche al fine di tutela preventiva: si pensi che, senza IP di destinazione, sarà davvero difficile per la stessa fornire una prova informatica a riscontro di quanto indicato in denuncia).
Nei fatti, in uno con le prescrizioni ai gestori da ultimo emanate dal Garante[14] e delle quali abbiamo traccia anche in questo procedimento, l'IP di destinazione viene ritenuto escluso – ai sensi del d.lgs. 109/2008 – dagli obblighi di conservazione e, quindi, immediatamente suscettibile di cancellazione.
O meglio, nell'incertezza interpretativa (tenendo ben presente anche il testo della Direttiva e non solo il suo recepimento nel testo di legge italiano) e a fronte delle sanzioni del Garante di cui al richiamato provvedimento del 17.01.2008, le società non lo conservano!
Infatti, a ben vedere, in tema di IP di destinazione si potrebbe sostenere anche il contrario: si consideri infatti come la previsione di cui all'art. 5 Direttiva non sia tassativa ma solamente indicativa di dati "non attinenti al contenuto delle comunicazioni" (i soli a non poter essere conservati a norma della Direttiva ai sensi dell'art. 5.2), anche perché l'originaria dizione restrittiva[15] per la quale «i tipi di dati da conservare per ciascuna delle categorie sopra menzionate sono specificati nell'allegato» era ormai scomparsa dal testo normativo comunitario.
In altre parole: l'IP di destinazione può ben considerato come uno dei «dati necessari per rintracciare e identificare la destinazione di una comunicazione» (art. 5 b Direttiva), nonostante lo stesso non venga poi espressamente menzionato ai successivi punti 1 e 2.
Una simile interpretazione, oltre a cogliere le osservazioni critiche di cui sopra, non avrebbe costituito in ogni caso una lesione alla riservatezza altrui, tenendo conto che neppure tale dato di per sé solo è in grado di restituire il contenuto della comunicazione.
E infatti, anche essendo a conoscenza di tale IP, in molti casi (che ricomprendono, quanto al panorama italiano, la quasi totalità degli accessi internet da rete fissa[16]) si sarebbe stati in grado di individuare non già «l'indirizzo internet delle pagine consultate o almeno delle relative homepage» ma solo quello della homepage: così si potrebbe ricavare – tramite interrogazione mediante semplici servizi reperibili in Internet – che all'indirizzo 130.186.85.14 corrisponde la pagina iniziale di www.giustizia.it. A questo punto, ma solamente con una ulteriore richiesta ai gestori di tale sito, si potrebbe tentare di risalire alla effettiva pagina visitata, sempre che le policy interne al manteiner (ovvero al soggetto deputato alla effettiva gestione delle pagine e alla loro allocazione sul server) prevedano la conservazione dei relativi log di navigazione dei visitatori
Si potrebbe controbattere, a questo punto, che anche l'informazione della semplice homepage visitata è già di per sé sufficiente ad integrare il paventato pericolo della riservatezza della navigazione.
E pur tuttavia dovranno essere prese in maggiore considerazione – nella disfida argomentativa e preso atto che nei sistemi NAT/PAT, senza l'indicazione dell'IP di destinazione, le richieste di files di log non servono a nulla (con enorme pregiudizio alle indagini, come nel caso in esame) – almeno due importanti considerazioni:
1) molto spesso – anche se edotti, con assoluta precisione, sulla pagina visitata dall'utente – si parla di una riservatezza che è già di per sé garantita dal fatto che trattasi di un soggetto potenzialmente non

---

d.lgs. 196/2003 ("Misure e degli accorgimenti a garanzia dell'interessato" attinenti alla conservazione dei dati del traffico telefonico e telematico per finalità di accertamento e repressione dei reati) – vengono comunque riproposti i riferimenti della Direttiva 2006/24/CE circa le categorie dei dati da conservare.

[13] Per meglio comprenderne l'impatto reale, è importante sapere che:

– il sistema NAT/PAT viene utilizzato, allo stato, da alcuni gestori telefonici che danno accesso alla rete internet da numerazioni fisse nonché da tutti coloro che offrono accesso al Web tramite connessioni da telefoni cellulari;

– le stesse reti aziendali o quelle della Pubblica Amministrazione sono configurate con sistemi NAT/PAT.

[14] Cfr. quanto emerge dal comunicato stampa reperibile su *http://www.garanteprivacy.it/garante/doc.jsp?ID=1481285*: sembrerebbe tuttavia che le maggiori problematicità siano limitate all'accesso ad Internet tramite l'uso di telefoni cellulari.

[15] Cfr. art. 4 della Proposta di Direttiva del 26.9.2005 pubblicata, con l'intero dossier normativo, in *http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=it&DosId=193330#375313*.

[16] Mentre oggi tutti i sistemi di accesso ad internet tramite cellulari, proprio perché gestiti in modalità NAT/PAT, erano teoricamente in grado di loggare non solo l'IP di destinazione ma anche la relativa URL (Uniform Resource Locator: sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet, come un documento o anche un'immagine) richiesta dall'utente.

identificabile dal semplice IP di origine.
L'IP di destinazione dunque, in ultima analisi e come già accennato, si rivela nel caso concreto un dato tendenzialmente non personale, stante la difficoltà ab origine di stabilire un preciso nesso tra l'identità dell'utente e gli indirizzi IP relativi alla propria navigazione web;
2) come mai una simile questione non è mai stata sollevata con riferimento alla numerazione telefonica del soggetto chiamato (dato peraltro espressamente indicato al punto 5.b.1 della Direttiva)?
Forse che l'informazione di una chiamata ad un particolare numero telefonico (si pensi, solo per rimanere nell'attualità delle indagini informatiche, a numerazioni a tariffazione maggiorata quale un 899 legato a servizi erotici) non possa ugualmente creare un pregiudizio in punto di riservatezza?
Ma, anche in questo caso, cosa in realtà è possibile davvero sapere – dal semplice numero telefonico chiamante – dell'effettivo interlocutore? O quale certezza è possibile avere, dal semplice numero telefonico chiamante, dell'effettiva conversazione intrattenuta (che, invece, può essere semplicemente frutto di un programma automatico cd. dialer che fa richiedere al personal computer collegato via modem alla linea telefonica, ad insaputa dell'utente, la connessione alla numerazione 899)?
Vero è, invece, che in entrambi i casi finora analizzati si ha a che fare con dati esterni alla comunicazione, che nulla dicono del contenuto della conversazione (quanto al numero telefonico del soggetto chiamato) o della navigazione (quanto all'IP di destinazione).
Senza considerare poi che la non conservazione dell'IP di destinazione vanifica[17], fin da subito, gran parte delle disposizioni della legge 6 febbraio 2006, n. 38 (in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet) e, in particolare, quelle relative agli obblighi per gli ISP di cui agli artt. 14-ter e 14-quater della legge 3 agosto 1998, n. 269[18].
Anche perché, se di sicurezza nella conservazione dei dati si vuole effettivamente parlare, basterebbe imporre una gestione separata – all'interno del medesimo ISP – dei database[19] relativi agli IP di origine e agli IP di destinazione: tale metodologia escluderebbe ab origine qualsiasi pericolo di interrelazione tra l'identità dell'utente e gli indirizzi IP relativi alla sua navigazione, con buona pace di tutti i soggetti interessati!

3) Quanto al problema del ***periodo di conservazioni dei dati relativi alle caselle di posta elettronica @hotmail.it****, questa Procura aveva già formalmente comunicato al Garante per la protezione dei dati personali – anche nell'ambito della consultazione pubblica avviata con la deliberazione del 19 settembre 2007[20] – il dato preoccupante che emergeva da alcune indagini svolte, preso atto dell'esistenza – oltre a casi di società italiane con server in Italia – di importanti società di diritto italiano (controllate tuttavia da società americane) aventi server all'estero.*
Orbene, a parere dello scrivente, siamo in presenza di società che trattano dati personali connessi alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione (cfr. art. 3 Direttiva n. 2002/58/CE[21]) e dunque, per tali motivi ed indipendentemente

---

[17] Si veda, sul punto, quanto recentemente riportato P. BIONDANI sul settimanale *L'Espresso*, 17 aprile 2008, 21: "Amato dimezzato. L'insanabile contrasto fra sicurezza e privacy è sfociato in uno scontro personale tra il ministero dell'Interno, Giuliano Amato, e il garante, Francesco Pizzetti. A margine dell'inaugurazione del centro della polizia postale contro la pedo-pornografia, varato in febbraio, tra Amato e Pizzetti sono volate parole grosse. Il casus belli è l'allargamento dell'obbligo di cancellazione dei dati telefonici e telematici imposto dall'Autorità garante della privacy. La legge Pisanu, varata nel 2005 dopo l'arresto in Italia di un terrorista di Londra tradito da un telefonino, prevedeva che le compagnie dovessero, al contrario, conservare i tabulati per esigenze di giustizia per almeno quattro anni (due per i computer). Appellandosi a una direttiva europea di imminente attuazione, invece, il garante ha dimezzato i termini: solo due anni per i telefoni, uno per i computer. Nel contrasto, la legge Pisanu, per una strana lacuna, non prevede sanzioni per chi non conserva, mentre il garante minaccia multe per chi non cancella. Risultato: compagnie come Vodafone, H3G e Wind stanno già annientando i dati. Di qui l'ira di Amato, condivisa da P.M. e poliziotti che indagano su mafia, terrorismo e pedofilia".

[18] Se ne riporta il testo, per comodità di lettura […].

[19] Oltre alla cd. segregation of duty, ovvero alla necessità che una sola persona non debba poter accedere ad entrambi i database.

[20] Il Dirigente del dipartimento attività ispettive e sanzioni presso il Garante per la protezione dei dati personali così conclude, 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, comma 2, 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, ancorché 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".

[21] Trattasi della Direttiva del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), pubblicata nella Gazzetta Ufficiale delle Comunità europee, 31.7.2002, L. 201/37.

In Internet all'indirizzo: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:IT:PDF*.

dalla allocazione dei relativi server, destinatarie degli obblighi precettivi della normativa (italiana e comunque comunitaria[22]) in materia di data retention.
Con la previsione dell'art. 5 d.lgs. 109/2008 (pubblicato nella Gazz. Uff. del 18 giugno 2008 n. 141), la questione assume ora una certa rilevanza, dal momento che vengono introdotte – a fronte di obblighi di conservazione dei dati, ***già esistenti nell'ordinamento italiano dall'estate del 2005*** *(negli stessi termini di 12 mesi in relazione ai dati del traffico telematico, così come introdotti dal cd. decreto Pisanu) – anche sanzioni amministrative per i relativi inadempimenti[23].*
Peraltro proprio il procedimento penale che aveva originato il richiamato invio degli atti all'Autorità Garante (trattandosi di violazione di misure minime di sicurezza in relazione ai sistemi informatici della società Yahoo! Italia, anch'essa con sede legale a Milano e avente i server negli USA presso la casa madre), era scaturito dall'impossibilità di fatto di concludere gli accertamenti di polizia giudiziaria alla luce di quanto denunciato dalla persona offesa in data 12.9.2005,[24] così come successivamente accertato dalla Guardia di Finanza – Gruppo Pronto Impiego di Milano (che ha condotto analoghi accertamenti anche in questa indagine, ad ausilio della Squadra reati informatici della Procura).
*All'esito dell'adempimento delle prescrizioni imposte dal Garante alla luce della contestazione mossa da questo Ufficio ai sensi dell'art. 169 d.lvo 196/2003, i legali della società in data 9 settembre 2008 avevano comunicato all'Autorità che Yahoo! Italia, "****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![25]) **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".*
Invero, e sebbene Microsoft notoriamente abbia nel suo core business anche l'attenzione alle problematiche investigative (con investimenti a favore della formazione e delle dotazioni informatiche delle forze di polizia), la documentazione fatta pervenire da Microsoft Corp e Macrosoft s.r.l. in questo procedimento è chiara nel senso che esse invece, ancor oggi e nonostante altri procedimenti penali conclusisi negativamente per lo stesso problema[26], non si considerano destinatarie degli obblighi di

---

[22] Cfr. art. 3 comma 2 Direttiva n. 2006/24/CE: «L'obbligo di conservazione stabilito al paragrafo 1 comprende la conservazione dei dati specificati all'articolo 5 relativi ai tentativi di chiamata non riusciti dove tali dati vengono generati o trattati e immagazzinati (per quanto riguarda i dati telefonici) oppure trasmessi (per quanto riguarda i dati Internet) da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione nell'ambito della giurisdizione dello Stato membro interessato nel processo di fornire i servizi di comunicazione interessati», e cioè – per il combinato disposto delle due Direttive – quelli di cui all'art. 3 Direttiva n. 2002/58/CE.

[23] Si riporta il testo della norma, per facilità di lettura [...].

[24] Si trattava 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 Presso, **datata 10 febbraio 2006**, considerato il periodo di conservazione dei files di log riguardante "solamente gli ultimi 30 giorni dalla data dell'accertamento") della casella di posta elettronica @yahoo.it in uso alla persona offesa.

[25] 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".

[26] Così l'annotazione di PG del 28.2.09: "Anche considerato che altri accertamenti di PG non hanno avuto riscontro positivo a causa del limitato periodo di conservazione dei dati applicato dalla Microsoft Corporation (si rimanda, ad esempio, al procedimento penale nr. 4722/07 R.G.N.R. mod. 44), si dava esecuzione alle deleghe d'indagine assegnate a questa P.G. che hanno portato all'acquisizione del materiale di seguito indicato, che viene allegato alla presente annotazione:

- comunicazione di Microsoft Corp. a firma di [...], con allegata traduzione del 23/10/2008, nella quale si evince che: "secondo la legge italiana, il servizio hotmail non è classificabile come servizio di comunicazione elettronica" e che "al momento manteniamo i dati relativi al traffico dei nostri 250 milioni di utenti per un periodo di 60 gg per supportare l'applicazione della Legge con le indagini attualmente svolte. Dal momento che mantenere una grande quantità di dati per un maggiore periodo di tempo comporterebbe problemi di natura tecnica, stiamo tuttora cercando una possibile soluzione tecnica affinché si possa mantenere i dati relativi al traffico degli utenti per un periodo di tempo maggiore". (**ALLEGATO 12**);
- esecuzione dell'ordine di esibizione atti e documenti presso Microsoft Srl del 19/12/2008 (**ALLEGATO 13**);
- verbale di assunzione informazioni rilasciate il 12/01/2009 da [...], Amministratore delegato di Microsoft s.r.l., nelle quali lo stesso si riporta "alla dichiarazione della […], peraltro, pervenuta da Microsoft Corp." e ribadisce "altresì, che Microsoft s.r.l., come soggetto giuridico, distinto da Microsoft Corp., non ha alcun potere di controllo in merito alle policy illustrate dalla stessa" (**ALLEGATO 14**).

conservazione qui indicati.
Considerato altresì che non esiste alcuna norma americana che impone un simile comportamento e che quindi tale policy appare esclusivamente dettata da ragioni economiche (tali da far sì che i costi d'impresa non sopportati si tramutino in sempre più elevati costi sociali, a fronte del pregiudizio che tale comportamento è idonee ad arrecare agli accertamenti di Polizia Giudiziaria), si procederà a trasmettere gli atti al Ministero dello sviluppo economico affinché contesti la violazione ed applichi la sanzione di cui all'art. 5 comma 2 D.lvo 30 maggio 2008, n. 109 (incompleta conservazione dei dati attinenti al traffico telematico in quanto per un periodo di gran lunga inferiore ai previsti 12 mesi).

4) Allo stato dunque rimangono solo dei meri indizi a carico di […], che non consentono tuttavia di sostenere ragionevolmente l'accusa in giudizio anche tenendo conto della facilità con la quale – oggigiorno – è possibile essere vittima di un furto di identità digitale o comunque di una sostituzione di persona.

La delicatezza della vicenda, data la notorietà e il ruolo istituzionale del destinatario delle affermazioni apparse sul blog, non deve tuttavia distogliere l'attenzione sul fatto che – laddove permanga tale stato di fatto e di diritto – qualsiasi altra indagine informatica tendenzialmente dovrà scontare le medesime difficoltà, con pregiudizio non solo per l'accertamento dei fatti ma anche per i diritti delle persone offese, tutte ugualmente meritevoli di tutela.

Il giudice per le indagini preliminari presso il tribunale di Milano Fabrizio D'Arcangelo fissava udienza ai sensi dell'art. 410 c.p.p. durante la quale, in data 9 luglio 2009, il pubblico ministero – nell'insistere nella richiesta di archiviazione – faceva presente che "con nota del 29 maggio 2009, successivamente alla richiesta di archiviazione sono stati trasmessi gli atti al ministero dello sviluppo economico affinché venga contestata la violazione, e applicata la sanzione, di cui all'art. 5 co. 2 D.L(gs) 30.5.2008 n. 109 a carico di Microsoft".

Sciogliendo la riserva, con provvedimento del 24.7.2009 il giudice disponeva ai sensi dell'art. 409 comma 4 c.p.p. il compimento di ulteriori indagini nel termine di sei mesi. In particolare, dopo una puntuale ricostruzione ed attenta analisi della normativa comunitaria e nazionale in materia di data retention,

- rilevava in generale come "il termine… per la conservazione dell'indirizzo IP di destinazione è certamente estraneo alla normativa comunitaria e nazionale e di certo non può essere introdotto in via amministrativa o per scelta di policy aziendale";
- indicava come non si potesse giungere a diversa soluzione (come affermato dal gestore H3G nella propria missiva di risposta alla PG) facendo leva sulle "prescrizioni adottate dal Garante per la Protezione dei Dati Personali in relazione ad alcuni gestori in data 10.1.2008" o sul "provvedimento generale in tema di 'sicurezza dei dati di traffico telefonico e telematico' emesso in data 17.1.2008" (quest'ultimo non disciplinando "espressamente il tema del termine di conservazione … dell'indirizzo IP per ragioni di giustizia");
- riteneva che "la linea interpretativa prospettata dal Garante per la Protezione dei Dati Personali nelle 'Prescrizioni sulla conservazione dei dati di traffico' adottate nei confronti di alcuni gestori in data 10.1.2008 non può essere condivisa" laddove essa afferma per i gestori l'obbligo di immediata cancellazione dell'indirizzo IP di destinazione, dal momento che "l'indirizzo IP di destinazione non può essere considerato di fatto coincidente con il 'contenuto della comunicazione'";
- preso atto che "l'art. 15 della Costituzione enuncia una riserva assoluta di legge" e "pertanto, le statuizioni del Garante per la Protezione dei dati Personali non possono delineare nel perimetro della categoria dei dati relativi al traffico telematico, in assenza di adeguato fondamento legale, una disciplina dell'indirizzo IP di destinazione difforme da quella prevista dal legislatore comunitario e

---

Nell'occasione l'Ufficio del PM dava atto che alle parti veniva mostrata una comunicazione della Yahoo! Italia s.r.l. – fornita, per conoscenza, all'Ufficio nell'ambito del Procedimento Penale 43083/07 mod. 21 – indirizzata al Garante per la protezione dei dati personali datata 9 settembre 2008, nella quale la stessa società dava atto 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 di traffico telematico […] per un periodo pari a 12 mesi;….". Preso atto di quanto sopra le parti chiedevano copia della documentazione mostrata e si riservavano eventualmente di produrre ulteriore documentazione a sostegno di quanto sinora esposto (documentazione poi fatta pervenire direttamente al Pubblico Ministero);

- accertamenti inerenti il servizio di posta elettronica @hotmail.it (**ALLEGATO 15**)".

> nazionale e, segnatamente, prevedere un termine inferiore di data retention rispetto a quello imposto dal legislatore comunitario e nazionale, o, addirittura, la sua immediata cancellazione", dichiarava *incidenter tantum* illegittime per competenza e violazione di legge e conseguentemente disapplicava "le prescrizioni adottate in *subiecta materia* dal Garante ed intese ad uniformare la disciplina dell'indirizzo IP di destinazione a quella del contenuto delle comunicazioni telematiche".

Tale decisione ebbe peraltro un notevole rilievo sugli organi di informazione[27], tanto da determinare una vibrante replica scritta ad opera della stessa autorità garante per la protezione dei dati personali[28].

Atteso che i dinieghi opposti alla procura di Milano da H3G e da Microsoft "non paiono avere alcun fondamento legale", il giudice per le indagini preliminari indicava al pubblico ministero, tra l'altro, il fatto che non vi fosse "alcuna evidenza agli atti che induca a ritenere irrimediabilmente compromessa la possibilità di acquisizione dell'indirizzo IP di destinazione di interesse", rilevando sul punto come "dalle comunicazioni agli atti non si evince se tale dato sia attualmente disponibile presso i gestori di servizi telematici o meno ed, in particolare, se tale dato sia comunque presente in copie di sicurezza (backup e disaster ricovery), essendo ignote le tecniche e le procedure informatiche adottare dai gestori per la cancellazione dei dati predetti".

Dopo gli ulteriori accertamenti eseguiti in ottemperanza di quanto indicato dal giudice per le indagini preliminari, in data 6 aprile 2010 il pubblico ministero reiterava la richiesta di archiviazione, sulla base delle seguenti argomentazioni:

RILEVATO CHE

> *Anche al fine di questa successiva richiesta di archiviazione, per facilità di esposizione verranno separatamente analizzati i due problemi già emersi in sede di indagini originariamente svolte e che possono essere così sintetizzati:*
>
> *A)* ***cancellazione degli IP di destinazione*** *ad opera dei gestori di telecomunicazione, ai sensi delle prescrizioni impartite dall'Autorità Garante prima dell'entrata in vigore del d.lgs 109/2008[29];*

---

[27] Cfr. L. FERRARELLA, *Blog anti-premier, il giudice vuole l'inchiesta*, in *Corriere della Sera*, 31 luglio 2009, p. 17. Cfr. anche dichiarazioni di L. BOLOGNINI, Presidente dell'Istituto Italiano Privacy, nel comunicato stampa del 1° agosto 2009 reperibile su *http://www.istitutoitalianoprivacy.it/it/2009/08/01/decisione-gip-milano-su-indirizzi-ip-istituto-privacy-prevedibile-la-divergenza-con-il-garante-serve-evoluzione-normativa.*

[28] "Internet: le norme sui dati personali. Con riferimento all'articolo «Blog anti-premier, il giudice vuole l'inchiesta» (Corriere, 31 luglio), desidero precisare che è del tutto infondata l'affermazione che il Garante abbia introdotto con proprio provvedimento a carico dei gestori telefonici l'obbligo di distruggere dopo due mesi i dati relativi agli indirizzi Ip degli utenti. In realtà il Garante, in stretta applicazione della legge e in conformità alla direttiva europea, ha affermato che i gestori telefonici hanno il diritto di detenere gli indirizzi Ip degli utenti solo relativamente al servizio di accesso alla rete da essi fornito. Di conseguenza ha dichiarato, sempre in applicazione di legge, illecita la conservazione degli indirizzi Ip relativi ad ogni altra attività svolta dagli utenti nell'uso della rete. È questo il quadro sulla base del quale l'Autorità ha stabilito l'obbligo per i gestori di distruggere tutti i dati relativi a indirizzi Ip in loro possesso diversi da quelli attinenti all'accesso alla rete. Il termine di due mesi di cui si parla nell'articolo è previsto nel provvedimento del Garante unicamente con riferimento al periodo concesso ai gestori per distruggere i dati da loro all'epoca illecitamente detenuti. Desidero sottolineare, infine, che la base giuridica del provvedimento del Garante prescinde del tutto dalla questione se gli indirizzi Ip debbano o meno essere considerati dati attinenti al contenuto della comunicazione": così Francesco Pizzetti, Presidente dell'Autorità Garante per la protezione dei dati personali, in *Interventi & Repliche*, Corriere della Sera, 2 agosto 2009, 39. Così invece la replica del giornalista Luigi Ferrarella: "Il gestore non deve mai conservare l'indirizzo Ip di destinazione, ribadisce il Garante, né per due mesi né per un minuto, e si basa sulla direttiva europea e sul codice in materia di protezione dei dati personali. Ma il provvedimento giudiziario, di cui ha riferito l'articolo, proprio dalla direttiva 2006/24/CE e dall'articolo 132 del codice ricava l'obbligo (per i gestori) di conservare il dato, rispettivamente, o per non meno di sei mesi e non più di due anni, o per un anno. I gestori sono disorientati, c'è chi ha speso 200 mila euro per attrezzarsi a obbedire al Garante e poi si è visto tirare le orecchie dai giudici. Forse gioverebbe una riflessione sull'assetto normativo. Anche per fugare il dubbio che le norme diano a chi delinque al computer (pedopornografia, truffe informatiche, cyberterrorismo) la possibilità di galleggiare in una bolla di impunità".

[29] Cfr. tra l'altro il parere richiesto all'Autorità Garante sullo schema di decreto legislativo volto a recepire la Direttiva 2006/24/CE, reso in termini favorevoli in data 5 marzo 2008 (e reperibile sul sito della Autorità: doc. web n. 1523089).

B) ***periodo di conservazione dei dati relativi alle caselle di posta elettronica @hotmail.it*** *da parte di Microsoft pari a 60 giorni, sulla base di una policy aziendale in contrasto con le disposizioni di legge vigenti (già esistenti nell'ordinamento italiano dall'estate del 2005, così come introdotte dalla Legge 31 luglio 2005, n. 155 di conversione del cd. decreto Pisanu, negli stessi termini di 12 mesi oggi previsti dal d.lvo 30 maggio 2008, n. 109 di attuazione della Direttiva n. 2006/24/CE in materia di data retention).*

Ebbene, anche alla luce delle ulteriori indagini compiute (delle quali si darà subito conto), non sono emersi elementi tali da consentire una identificazione certa dell'autore delle e-mail a carattere criminoso oggetto del presente procedimento.

*A) Con provvedimento del 27.7.2009 veniva immediatamente disposta l'ispezione dei sistemi informatici nella disponibilità di H3G, sul presupposto che "****al fine di identificare l'IP di destinazione – per il periodo compreso dalle ore 18,30 alle ore 19,00 del giorno 09/06/2008 – relativamente all'IP NAT. 62.13.173.176,*** *è assolutamente indispensabile la cristallizzazione delle informazioni allocate sui sistemi informatici ....., ****anche ove le stesse siano state cancellate o comunque possano essere reperite mediante incrocio di dati detenuti su supporti di backup o reperibili su registri cartacei (eventualmente trattenuti dalla società ai fini civilistici, ai sensi dell'art. 123 D.Lgs. 30.6.2003 n. 196 – Codice in materia di protezione dei dati personali)****, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".*
Gli esiti di tale attività sono compendiati nel verbale di operazioni compiute in data 29.7.2009 (presso la sede legale di H3G in Roma) e 30.7.2009 presso il luogo ove sono materialmente ubicati i server interessati (apparecchiature fornite da Fastweb ad H3G, tramite apposito contratto di housing, ed ubicate a Milano, [...] – con gestione da remoto dalla sede di Segrate della [....] società che gestisce in outsourcing i sistemi informativi di H3G): in tale occasione la Polizia Giudiziaria aveva modo di accertare definitivamente come

il sistema CRS, sistema utilizzato per loggare i dati di traffico internet fino all'ottobre 2008 non era più disponibile perché dismesso e, dopo la cancellazione dei dati in esso contenuti, le apparecchiature che lo costituivano sono state assegnate ad altri progetti.

Peraltro, come emerso anche dalle dichiarazioni di [....] ***nel periodo di interesse gli IP di destinazione, in adesione alle prescrizioni del Garante****,* ***non venivano neppure memorizzati sui server.***
Più precisamente:

l'azienda utilizzava, sino a prima delle disposizioni del Garante, un sistema, denominato CRS, il quale decodifica i dati grezzi e produce i tabulati di traffico telematico. Tale sistema acquisiva l'IP di destinazione. Successivamente all'emanazione delle disposizioni del Garante è stata inibita l'acquisizione dell'IP di destinazione ed è iniziata un'attività di cancellazione dei dati in argomento per tutti i dati di specie presenti sul sistema detenuti ai fini della data retention per l'Autorità Giudiziaria. Pertanto, considerato che tale attività comportava un enorme dispendio di risorse, l'azienda ha implementato una nuova tecnologia che non acquisisce il dato. Preciso che per le attività di cancellazione e tutte quelle di adeguamento tecnico della rete di comunicazione il costo sostenuto dall'azienda per tale implementazione è stato di circa 200.000,00 euro a questi vanno aggiunti i costi sostenuti per adeguare il sistema HTS di cui non conosco gli importi. Preciso ancora, riallacciandomi a quanto detto prima, che a far data dal 10.03.2008 l'IP di destinazione non veniva più acquisito dal sistema e, in pari data, sono contestualmente iniziate le operazioni di cancellazione dei dati di specie su quelli antecedenti. Tale operazioni di cancellazione sono terminate nel mese di luglio 2008 *(dichiarazioni rese dal […], responsabile Ingegneria sistemi di gestione Rete H3G);*

l'azienda è stata oggetto di un'ispezione, a inizio 2008, dell'Autorità Garante sulla protezione dei dati personali la quale ha imposto, ai sensi dell'art. 154 comma 1 lettera d) del Codice di merito; la cancellazione, tra le altre cose, dell'IP di destinazione dando all'azienda un termine di 60 giorni per l'adeguamento a tale disposizione[30]. Quindi, riepilogando, sino ai primi del 2008 gli indirizzi IP di destinazione venivano conservati e, successivamente, con decorrenza marzo 2008, non solo tali dati non

[30] La PG dava atto che tale documentazione veniva esibita ed allegata al verbale.

vengono più conservati ma, da tale data, gli stessi non vengono nemmeno registrati[31] *(dichiarazioni rese dal […], responsabile Ufficio Prestazioni Obbligatorie H3G);*

nel 2008 era presente una piattaforma denominata CRS, piattaforma che ha cessato di funzionare nell'ottobre del 2008. Fino al marzo del 2008 questa piattaforma registra anche l'IP di destinazione della navigazione internet dell'utente ed anche l'url della pagina web visita. Con l'emanazione da parte del Garante per la Privacy del 10 gennaio 2008, del provvedimento che imponeva ad H3G di non conservare i dati di navigazione, è stata eliminata la possibilità di formazione del dato a partire dal 10 marzo 2008 e da tale data si è avviato il processo di cancellazione dei dati che sino ad allora erano stati conversati. Quest'ultimo processo di cancellazione è terminato il 16 luglio 2008.
Contemporaneamente era attiva la piattaforma denominata HTS che sin dall'origine non prevedeva l'acquisizione dell'IP di destinazione (url di visita). Proprio per questo motivo, per soddisfare la normativa in vigore prima del 10 gennaio 2008, ovvero l'indicazione dell'IP di destinazione, era necessario l'utilizzo della piattaforma CRS che forniva i dati per la composizione dei file di log eventualmente richiesti dall'A.G..
In quel periodo le due piattaforme sono rimaste in funzione parallelamente.
A partire dal 3 settembre 2008 è stata implementata l'infrastruttura di firewall che permettere di inviare al sistema HTS le informazioni necessarie per consentire l'associazione univoca tra l'IP pubblico e l'IP privato del cliente H3G che effettua la navigazione.
Il 22 ottobre 2008 viene quindi materialmente dismessa la piattaforma CRS, senza alcuna migrazione o conservazione di dati in quanto quelli necessari erano completamente contenuti nella piattaforma HTS.
Dopo una attività di cancellazione dei dati contenuti, peraltro dati che venivano immagazzinati in formato crittografato, la partizione dei server destinata alla piattaforma CRS è stata riutilizzata per altri progetti, i cui dati sono andati, comunque, a sovrascrivere quelli che eventualmente erano ancora residente sui dischi. Un'operazione di data recovery su tale partizione, peraltro impossibile, darebbe comunque come risultato, dopo operazione di ricostruzione del dato grezzo, fornirebbe le stesse informazioni trasmesse ed acquisite dall'A.G. *(dichiarazioni rese dal […], responsabile Ericsson Network Services Italia per la Governance Security di H3G)*

Per restituire al Giudice per le indagini preliminari una visione complessiva della problematica sottesa, in data 15.09.2009 si procedeva altresì ad acquisire sommarie informazioni testimoniali da […], dal settembre 2004 responsabile Ufficio Rapporti con l'AG di Fastweb: infatti la richiamata società, pur non essendo stata destinataria dei provvedimenti del Garante del 10.1.08, era stata tra le prime in Italia ad utilizzare le reti NAT la cui struttura (e i relativi problemi per le investigazioni) è analoga a quelle in uso, all'epoca dei fatti, da H3G.
Sul punto lo stesso dichiarava:

Dopo l'entrata in vigore del decreto cd. Pisanu, con investimenti da parte nostra avendo una rete NAT che all'epoca non teneva alcuna traccia delle connessioni, ci siamo messi in regola con i prescritti obblighi di tracciamento e conservazione a partire dal luglio 2006. Da quel momento tracciavamo e conservavamo anche l'IP di destinazione, essendo la normativa chiara sul punto.
Quando l'Autorità Garante per la protezione dei dati personali, nel gennaio 2008, ha sanzionato alcuni operatori nazionali (TIM, VODAFONE, H3G) abbiamo ritenuto, d'intesa con l'Ufficio legale interno, di adottare la stessa linea interpretativa che traspariva da tali disposizioni, ovvero che l'IP di destinazione dovesse essere considerato come parte della comunicazione e quindi immediatamente cancellato. Più precisamente, abbiamo adeguato i nostri sistemi, con ulteriori investimenti, affinché l'IP di destinazione, appena instradata la comunicazione, venisse cancellato e quindi mai conservato presso i nostri server.
A seguito dell'entrata in vigore del d.lvo 109/2008 e successive proroghe sul punto, con ulteriori investimenti abbiamo ristrutturato l'intera nostra architettura di rete al fine di consentire la prescritta "identificazione univoca dell'utente": questo è avvenuto a partire dalla fine di marzo 2009.
Quindi, allo stato, siamo in grado di rispettare le prescrizioni del richiamato decreto legislativo, conservando i dati per finalità di accertamento e di giustizia per 12 mesi e in maniera tale da consentire il tracciamento certo dell'origine della connessione. Dopo tale periodo, i dati vengono cancellati.
Possiamo quindi restituire, ai fini di giustizia, solamente il dato relativo all'ingresso sulla nostra rete (ovvero i dati relativi all'utilizzatore della risorsa) e non quello relativo alle attività compiute per il tramite della nostra rete.

[31] La PG dava atto che veniva esibita ed allegata al verbale la risposta formale comunicata al Garante in ottemperanza a quanto da questi disposto.

Come già indicato nella originaria richiesta di archiviazione, appare dunque evidente come, sulla base delle già richiamate prescrizioni del Garante datate 10.1.2008 e 17.1.2008, di fatto si è proceduto ad una indebita cancellazione di dati utili per il proseguo delle investigazioni penali.
E ciò con ***effetti irreversibili e pregiudizievoli, per le indagini in corso, per un periodo temporale davvero significativo*** *(dal 10 gennaio 2008 – a seguito della immediata ottemperanza ad opera di tutti i gestori italiani, attese le ingenti sanzioni pecuniarie correlate ad una eventuale inosservanza – e quantomeno fino alla data di completa adesione, ad opera dei medesimi gestori, al meccanismo dell'"assegnazione di un IP in maniera univoca", così come oggi previsto dall'art. 6 comma 5 d.lvo 109/08[32] e sanzionato dall'art. 5 comma 2 stesso d.lvo).*

Come correttamente richiamato dal GIP, ***l'origine della impostazione volta ad equiparare l'IP di destinazione ad un dato attinente il "contenuto della comunicazione" deve ritrovarsi nello stesse motivazioni alla base del provvedimento del Garante del 10.1.2008*** *emanato nei confronti di H3G[33]:*

Per il traffico telematico, peraltro, vista la particolarità delle informazioni trattate, si pongono specifiche criticità rispetto alle comunicazioni telefoniche, potendosi non di rado riscontrare una sostanziale identificazione fra il dato esteriore della comunicazione elettronica e il contenuto della stessa. **Alcuni dati di traffico telematico, apparentemente "esterni" alla comunicazione elettronica (come, ad esempio, le pagine web visitate o gli indirizzi Ip di destinazione), coincidono di fatto, nella maggior parte dei casi, con il "contenuto" della comunicazione medesima**, consentendo, tra l'altro, di ricostruire direttamente o indirettamente relazioni personali e sociali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute.

Il richiamato provvedimento del Garante disponeva, ai sensi dell'art. 154 comma 1 lett. d) Codice Privacy e "nei termini di cui in motivazione"

il divieto della conservazione, in qualsiasi forma e grado di dettaglio, di informazioni sui siti visitati dagli utenti, anche qualora esse siano specificate con notazione Url o con mero indirizzo Ip di destinazione; dispone, per l'effetto, la cancellazione dei dati trattati illecitamente al più presto, dando riscontro a questa Autorità dell'avvenuta cancellazione entro e non oltre il termine di sessanta giorni dalla data di ricezione del presente provvedimento;

Nello stesso senso (ed anzi, ad essere più precisi, utilizzando le stesse parole quanto alle richiamate motivazioni), tuttavia, anche i provvedimenti di pari data emanati nei confronti di Vodafone[34] e Telecom Italia[35]: tale interpretazione quindi sta alla base delle prescrizioni impartite ai richiamati gestori, come peraltro confermato dai richiamati testi sentiti ad integrazione delle indagini.

Con tali provvedimenti l'Autorità Garante di fatto introduce, per la prima volta nel nostro ordinamento, una categoria di dati del traffico telematico da non conservare (in contrasto con le vigenti disposizioni di legge)*. E in effetti, con la originaria richiesta di archiviazione, si era significativamente segnalato il passaggio della relazione annuale per il 2007 del Garante (p. 6) proprio a commento dei richiamati provvedimenti del 10.1.2008:*

i gestori **devono infatti conservare esclusivamente i dati di traffico telematico funzionali alla fornitura e alla fatturazione del servizio di connessione e non i dati di traffico apparentemente "esterni" alla comunicazione (pagine web visitate o gli indirizzi Ip di destinazione) e che possono peraltro coincidere di fatto con il "contenuto" della comunicazione**, consentendo di ricostruire meglio relazioni personali e sociali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute.

Ma vi è di più…..

---

[32] Si riporta, per facilità di lettura, il testo: "*I fornitori di servizi di comunicazione elettronica accessibili al pubblico che offrono servizi di accesso a internet (Internet Acces Provider) assicurano la disponibilità e l'effettiva univocità degli indirizzi di protocollo internet entro novanta giorni dalla data di entrata in vigore del presente decreto*".

[33] Il grassetto, in questo e negli altri richiami a provvedimenti/testi dell'autorità garante, è del pubblico ministero.

[34] Reperibile sul sito della Autorità: doc. web n. 1484758.

[35] Reperibile sul sito della Autorità: doc. web n. 1524263.

Tale interpretazione, infatti, ricorre espressamente anche nelle "considerazioni preliminari" del provvedimento a carattere generale del 17.1.2008, ove appunto si legge:

Il trattamento dei dati di traffico telefonico e telematico presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

Tali informazioni hanno una natura particolarmente delicata e la loro impropria utilizzazione può avere importanti ripercussioni sulla sfera personale di più soggetti interessati; possono avere un'"accentuata valenza divulgativa di notizie caratterizzanti la personalità dell'autore" e la loro conoscibilità richiede adeguate garanzie (cfr., fra l'altro, Corte cost. 11 marzo 1993, n. 81 e 14 novembre 2006 n. 372).

I dati relativi al traffico telefonico e telematico dovrebbero peraltro riguardare solo alcune caratteristiche esteriori di conversazioni, chiamate e comunicazioni, senza permettere di desumerne i contenuti.

Inoltre, le stesse caratteristiche esteriori permettono di individuare analiticamente quando, tra chi e come sono intercorsi contatti telefonici o per via telematica, o sono avvenute determinate attività di accesso all'informazione in rete e persino il luogo dove si trovano i detentori di determinati strumenti.

L'intensità dei flussi di comunicazione comporta la formazione e, a volte, la conservazione di innumerevoli informazioni che consentono di ricostruire nel tempo intere sfere di relazioni personali, professionali, commerciali e istituzionali, e di formare anche delicati profili interpersonali. Ciò, specie quando i dati sono conservati massivamente dai fornitori per un periodo più lungo di quello necessario per prestare servizi a utenti e abbonati, al fine di adempiere a un distinto obbligo di legge collegato a eccezionali necessità di giustizia.

Per le comunicazioni telematiche, poi, si pongono ulteriori e più specifiche criticità rispetto alle comunicazioni telefoniche tradizionalmente intese, in quanto il dato apparentemente "esterno" a una comunicazione (ad es., una pagina web visitata o un indirizzo Ip di destinazione) spesso identifica o rivela nella sostanza anche il suo contenuto: può permettere, quindi, non solo di ricostruire relazioni personali e sociali, ma anche di desumere particolari orientamenti, convincimenti e abitudini degli interessati.

Eventuali abusi (quali quelli emersi nel recente passato, allorché sono stati constatati gravi e diffusi fatti di utilizzazione illecita di dati), possono comportare importanti ripercussioni sulla sfera privata degli individui o anche violare specifici segreti attinenti a determinate attività, relazioni e professioni.

Emerge quindi la necessità, in attuazione di quanto previsto per legge, di assicurare che la conservazione di tali dati da parte dei fornitori, laddove essa sia necessaria per prestare un servizio o in quanto imposta dalla legge, avvenga comunque in termini adeguati per garantire una tutela maggiormente efficace dei diritti e delle libertà delle persone.

Per tali motivi, a prescindere dalle garanzie previste in termini più generali nell'ordinamento anche sul piano costituzionale e processuale, **il legislatore all'art. 132 del Codice ha demandato al Garante per la protezione dei dati personali l'individuazione delle misure e degli accorgimenti che i fornitori dei servizi di comunicazione elettronica devono adottare a fronte della conservazione dei dati di traffico telefonico e telematico, allo stato prescritta per finalità di accertamento e repressione dei reati.**

Il presente provvedimento è rivolto appunto a individuare le elevate cautele che devono essere osservate dai fornitori nella formazione e nella custodia dei dati del traffico telefonico e telematico.

Prima di indicare quali cautele risultano necessarie a seguito del complesso procedimento di accertamento curato dal Garante, sono opportune alcune altre premesse sull'attuale quadro normativo, sui fornitori e sui dati personali coinvolti.

Peraltro, da quanto sopra riportato, era evidente alla stessa Autorità Garante come ***l'art. 132 comma 5 Codice Privacy (nella versione allora in vigore, prima della modifiche introdotte dal d.lvo 196/2008)***

demandi ad essa compiti – quali quello di individuare misure e accorgimenti che i fornitori dei servizi di comunicazione elettronica devono adottare a fronte della conservazione dei dati del traffico – completamente diversi dall'introdurre ipso iure categorie di dati del traffico da conservare/non conservare.
E tuttavia proprio tramite il richiamato provvedimento del 17.1.2008 l'Autorità Garante ribadiva, questa volta introducendo surrettiziamente tale interpretazione a livello generale, l'indirizzo IP di destinazione quale categoria di dati del traffico telematico da non conservare.

Che anche tale provvedimento a carattere generale si muova al di fuori dell'allora vigente impianto normativo (costituito dall'art. 132 d.lvo 196/2003 così come modificato dalla Legge 155/2005: così sul punto anche il par. 2.2. del provvedimento del 17.1.2008) forse apparve chiaro allo stessa Autorità Garante quando, in data 24 luglio 2008, fu costretta ad emanarne un successivo di modifica[36]*:*

VISTO il decreto legislativo 30 maggio 2008, n. 109, di recepimento della direttiva 2006/24/Ce del Parlamento europeo e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/Ce; visto, in particolare, l'art. 2 di tale decreto che ha modificato nuovamente l'art. 132 del Codice;

CONSIDERATO che è ora previsto un periodo unico di conservazione pari a 24 mesi per i dati di traffico telefonico, a 12 mesi per i dati di traffico telematico e a 30 giorni per i dati relativi alle chiamate senza risposta, senza distinzioni in base al tipo di reato;

In esso peraltro viene rilevata:

la necessità di apportare al menzionato provvedimento generale alcune modifiche strettamente necessarie in ragione delle **suindicate novità di carattere normativo riguardanti la durata della conservazione dei dati, nei termini di cui al seguente dispositivo, dando atto che il medesimo provvedimento del 17 gennaio 2008 resta immutato per ogni altro profilo**;

laddove invero, nella stessa relazione al Parlamento[37] *circa l'attività svolta nel 2008, così si legge (p. 31):*

Il decreto legislativo – sul cui schema l'Autorità ha reso un parere (*v. supra*) – ha individuato termini di conservazione di tali dati più proporzionati e rispondenti alla normativa comunitaria, individuando un periodo unico di conservazione per ciascuna categoria di dati, senza ulteriori distinzioni in base al tipo di reato, pari a ventiquattro mesi per i dati di traffico telefonico e a dodici mesi per i dati di traffico telematico (art. 132, comma 1, del Codice). Lo stesso decreto ha, inoltre, stabilito in trenta giorni il periodo di conservazione dei dati relativi alle *"chiamate senza risposta"* (art. 132, comma 1-*bis*, del Codice). […]

Il d.lg. n. 109/2008, con autonome disposizioni, ha inoltre individuato le categorie di dati di traffico telefonico e telematico oggetto di specifica conservazione e disciplinato, anche con norme transitorie, l'obbligo per i fornitori di servizi di comunicazione elettronica di conservare i dati relativi alle chiamate senza risposta e al *cd. "indirizzo Ip"* univocamente assegnato, indispensabile per individuare i soggetti che accedono a Internet. […]

Al riguardo, è importante ricordare che, nel corso dei lavori di conversione del d.l. n. 151/2008, il Governo ha accettato un ordine del giorno della Camera con il quale si è impegnato a favorire ogni iniziativa diretta ad assicurare l'univocità degli indirizzi IP, sollecitando i fornitori di servizi di comunicazione elettronica che offrono servizi di accesso ad Internet (*Internet access provider*) ad adoperarsi al più presto per garantire detta prestazione nell'interesse della giustizia (o.d.g. 9/1857/7). Tale ordine del giorno è il frutto anche

[36] Reperibile sul sito della Autorità: doc. web n. 1538224.

[37] Reperibile sul sito della Autorità: doc. web n. 1632972.

della collaborazione prestata dall'Autorità ad un apposito tavolo di lavoro organizzato presso il Ministero dell'interno.

Infine, il d.lg. n. 109/2008, in attuazione di specifiche previsioni della direttiva, ha:

[…]

– precisato che il Garante esercita il controllo sul rispetto della disciplina in materia di protezione dei dati personali anche *"con riferimento alla conservazione dei dati di traffico"* (art. 154, comma 1, lett. a), del Codice);

– introdotto specifiche fattispecie sanzionatorie in materia di conservazione di dati di traffico (art. 162-*bis* del Codice; art. 5, comma 2, d.lg. n. 109/2008).

Dunque, come emerge anche dalle complessive affermazioni dello stesso Garante, il d.lvo 109/2008 non ha inciso solamente sui ***termini****, anche, sulle* ***categorie di dati*** *oggetto di conservazione (e sui consequenziali obblighi di cancellazione per i dati non ricompresi in tali categorie).*

Invero, il regime previgente l'attuazione della Direttiva 2006/24/CE era ben noto all'Autorità Garante: ed infatti, a rileggere il testo del provvedimento del 17.1.2008 alla luce delle considerazioni del Giudice per le indagini preliminari, appare significativa l'impostazione metodologica seguita dal Garante in quanto espressamente dichiarata al par 2.3:

Al fine di armonizzare le disposizioni degli Stati membri sul tema della conservazione dei dati di traffico per finalità di accertamento e repressione di reati è poi intervenuta la direttiva n. 2006/24/Ce del Parlamento europeo e del Consiglio del 15 marzo 2006, che doveva essere recepita entro il 15 settembre 2007.

Tale direttiva contiene specifiche indicazioni sul risultato convenuto a livello comunitario con riferimento sia ai tempi di conservazione dei dati di traffico (minimo sei mesi e massimo due anni), sia alla corretta e uniforme individuazione delle "categorie di dati da conservare" (analiticamente elencate nell'art. 5 della direttiva medesima); ciò, in relazione agli specifici servizi ivi enucleati, ovvero di telefonia di rete fissa e di telefonia mobile, di accesso a Internet, di posta elettronica in Internet e di telefonia via Internet.

In questo quadro risulta necessario tenere conto di tali indicazioni anche nell'ambito del presente provvedimento. Ciò, anche in considerazione del fatto che nell'attuale quadro normativo interno, pur sussistendo una definizione generale di "dati relativi al traffico" (art. 4, comma 2, lett. h) del Codice), tali dati non vengono enumerati, né vengono distinti espressamente i dati relativi al traffico "telefonico" da quelli inerenti al traffico "telematico".

Se questo dunque era l'intento dichiarato dell'Autorità, non si possono che condividere gli elementari principi di diritto doverosamente ricordati dal Giudice per le indagini preliminari nelle motivazioni che hanno determinato la disapplicazione dei provvedimenti del Garante in subiecta materia.

Peraltro, in simile contesto, davvero non si comprende la ricostruzione della vicenda così come fatta ufficialmente pervenire agli organi di stampa dal Presidente dell'Autorità Garante:

"[…] il Garante, in stretta applicazione della legge e in conformità alla direttiva europea, ha affermato che i gestori telefonici hanno il diritto di detenere gli indirizzi Ip degli utenti solo relativamente al servizio di accesso alla rete da essi fornito. Di conseguenza ha dichiarato, sempre in applicazione di legge, illecita la conservazione degli indirizzi Ip relativi ad ogni altra attività svolta dagli utenti nell'uso della rete. È questo il quadro sulla base del quale l'Autorità ha stabilito l'obbligo per i gestori di distruggere tutti i dati relativi a indirizzi Ip in loro possesso diversi da quelli attinenti all'accesso alla rete. ……. Desidero sottolineare, infine, che la base giuridica del provvedimento del Garante prescinde del tutto dalla questione se gli indirizzi Ip debbano o meno essere considerati dati attinenti al contenuto della comunicazione […]".

Più in linea con la realtà dei fatti sono invece le parole del Presidente dell'Istituto Italiano per la Privacy (IIP), le cui conclusioni rispecchiano, amaramente, quelle già indicate dal Pubblico Ministero al termine della originaria richiesta di archiviazione:

"Che l'IP sia o meno un dato personale non rileva nella discussione in esame. L'indirizzo IP di destinazione (da non confondere con l'IP d'accesso) e gli indirizzi dei siti web visitati dagli utenti sono considerati dal Garante sia dati di traffico sia dati di contenuto (e quindi potenzialmente sensibili): per tale ragione, interpretando la Direttiva 2006/24/CE e l'articolo 132 del nostro Codice Privacy, il Garante decise nel senso che, essendo quei dati anche delicate informazioni personali, troppo "lontani" dall'operatore per essere ricompresi nel suo dominio e dunque non solo indicatori di traffico telematico, andassero esclusi dall'obbligo di conservazione per ragioni di accertamento e repressione dei reati (obbligo previsto nella normativa nazionale e comunitaria per i soli dati di traffico). L'autorità amministrativa, nel suo provvedimento del 2008, stabilì cioè che dovesse prevalere la loro natura di contenuti sensibili secondari piuttosto che quella di "dati di traffico" che pur tuttavia avevano. Fu un'interpretazione estensiva della tutela privacy, a nostro parere non del tutto coperta da norme primarie: ci troviamo infatti innanzi ad un parziale silenzio legislativo, e adesso come prevedibile un primo magistrato ha rilevato i limiti della regolazione secondaria.
Come IIP, chiediamo quanto prima integrazioni a livello europeo della Direttiva 2006/24/CE e quindi, di conseguenza, dell'art. 132 del nostro Codice, che chiariscano che l'obbligo di conservazione, per fini d'accertamento e repressione dei reati, è esteso ai dati di traffico che siano anche, seppur non solo, informazioni di contenuto (come l'IP di destinazione o gli indirizzi dei siti) ed inoltre sottopongano i content providers ai medesimi obblighi di conservazione ora previsti per i fornitori di servizi di comunicazione elettronica. È vero che, come Istituto, il nostro obiettivo è contribuire a salvaguardare la privacy dei cittadini: ma senza garanzie di rintracciabilità dei responsabili di crimini commessi on line diventa impossibile anche proteggere i dati personali degli utenti e si arriva al paradosso di tutelare i delinquenti anziché le vittime di reati su internet."

A questo punto, più che un "ripensamento" dell'Autorità Garante, appare urgente in materia l'intervento del Legislatore: ed infatti la disapplicazione dei richiamati provvedimenti del Garante non è di per sé sola in grado di scrivere la parola fine alla vicenda interpretativa, dal momento che – ***anche per gli ingenti investimenti economici finora effettuati dai gestori per adeguarsi alle prescrizioni ivi dettate – gli IP di destinazione a tutt'oggi continuano di fatto ad essere cancellati dai gestori.***
E dunque, anche se oggi trova applicazione – ad opera della maggior parte dei gestori – l'assegnazione dell'IP (di origine) in maniera univoca così come previsto dall'art. 6 comma 5 d.lvo 109/08, [….] per i gestori è possibile trasmettere alla Autorità Giudiziaria, "ai fini di giustizia, solamente il dato relativo all'ingresso sulla nostra rete (ovvero i dati relativi all'utilizzazione della risorsa) e non quello relativi alle attività compiute per il tramite della nostra rete)".
Per rendere meglio l'idea ***sarebbe come se, ad un tratto, il gestore telefonico si limitasse a fornire alla Autorità Giudiziaria, con i relativi tabulati del traffico, i dati relativi al solo numero chiamante, omettendo di comunicare i numeri telefonici da esso chiamati****!*
È quindi non solo lecito ma anche doveroso (ai fini di una più efficace tutela delle vittime di reati su Internet) dubitare che un sistema siffatto, quanto alla conservazione dei dati del traffico telematico a fini di giustizia, sia effettivamente conforme alla ratio della Direttiva 2006/24/CE…

B) quanto al profilo attinente Microsoft, non si è proceduto ad emettere analogo provvedimento di ispezione dei server interessati dal momento che, anche alla luce della esperienza investigativa del pool reati informatici della Procura di Milano, è pacifico la loro allocazione all'estero.
Peraltro, come già avvenuto in relazione ad altri gestori aventi server negli USA, anche l'espletamento di una rogatoria così come avvenuto tempestivamente in altre indagini[38] *ha dato esiti negativi, attesi i tempi*

[38] Nelle fasi iniziali di una importante indagine relativa ad una organizzazione transazionale (pp. 47258/05 R.G.N.R. mod. 44) dedita al phishing, in data **15 giugno 2006** vennero in primis richiesti – con decreto del Pubblico Ministero – i dati relativi agli intestatari di una e-mail @yahoo.com direttamente alla sede legale di Yahoo! Italia in Milano. Due giorni dopo pervenne la seguente risposta: "Riscontriamo la Vostra del 16 giugno u.s. concernente la questione in oggetto per significarVi che siamo nell'impossibilità materiale di dare seguito alla Vostra richiesta in quanto Yahoo! Italia non offre né gestisce il servizio di posta elettronica "web based" avente l'account @yahoo.com che è invece offerto e gestito dalla società Yahoo! Inc., società costituita ai sensi della legge del Delaware con sede principale a 701 First Avenue, Sunnyvale, CA 94089 0703, USA. Si rende pertanto per Voi necessario, al fine di ottenere le richieste informazioni di rivolgerVi direttamente, nelle forme e modi di rito, all'anzidetto soggetto giuridico titolare dei rispettivi servizi. Peraltro, la richiesta de qua necessita, per essere processata correttamente, di essere istruita tramite rogatoria internazionale rivolta all'Autorità Americana competente". Solo in data **12 marzo 2007**, all'esito della rogatoria formalmente inoltrata, è pervenuta la

stretti di conservazione ivi vigenti (di regola inferiori a quelli necessari per l'esecuzione di simili richieste di assistenza giudiziaria).
Nonostante la rilevanza[39] e l'attualità del tema portato all'attenzione del Ministero dello Sviluppo Economico – Direzione Generale per i Servizi di Comunicazione Elettronica e Radiodiffusione (quale Autorità competente ai sensi dell'art 5 comma 2 D.lvo 30 maggio 2008, n. 109), deve registrarsi come – a quasi un anno di distanza dalla trasmissione dei relativi atti e nonostante il formale sollecito in data 22.2.2010 (cfr. atti allegati) – non è pervenuta alla Procura di Milano la comunicazione di alcun tipo di determinazione sul punto.

Solo in data 19 aprile 2010 perveniva alla procura di Milano la risposta del ministero dello sviluppo economico, nella quale si faceva presente che

il servizio considerato non sembra riferibile alla gestione da parte della Microsoft S.r.l. […]

La soluzione della problematica di cui trattasi presenta un'indubbia complessità e risente della mancanza di accordi tra lo Stato Italiano e gli Stati di appartenenza (in questo caso gli U.S.A.) delle imprese in grado di conservare e mettere a disposizione i dati del traffico telematico relativo ai propri utenti […].

Dal momento che la società ha sede all'estero, non trova applicazione il disposto di cui al decreto legislativo 109/2008 in materia di data retention […].

Infine si aggiunge che la società Microsoft, da quanto è dato rilevare dagli atti del procedimento per l'accertamento del reato in data 9 giugno 2008, avrebbe messo a disposizione i dati del traffico relativi ai due mesi precedenti la richiesta ma non i dati relativi al periodo ulteriormente anteriore (al quale quindi si riferirebbe il mancato rispetto dell'obbligo e l'applicazione della sanzione). Tuttavia nel periodo in questione (e comunque prima del 3 luglio 2008), per quanto operasse già un obbligo a carico degli operatori soggetti alla legge italiana, il decreto legislativo 109/2008 non era entrato in vigore […] Anche per tali motivi, ne sarebbe dubbia l'applicabilità.

Essa veniva trasmessa al giudice delle indagini preliminari con le seguenti osservazioni del pubblico ministero:

*Nonostante la riconosciuta "*indubbia complessità*" della problematica sottoposta alla attenzione del Ministero, l'allegata risposta pare limitarsi ad affermare – in tre righe apodittiche – come la riconducibilità del servizio di posta elettronica @hotmail.it debba essere individuata (esclusivamente) in capo a Microsoft Corporation, senza dar conto degli argomenti contrari complessivamente evidenziati nella nota di questa Procura datata 29 maggio 2009 (1. rilevanza del luogo ove i servizi Internet vengono offerti, come da consolidata giurisprudenza non solo europea ma anche americana; 2. formale riconducibilità in ambito UE del rapporto relativo al servizio di posta elettronica @hotmail.it, come evidente dalla mera lettura delle stesse clausole contrattuali; registrazione del sito hotmail.it ad opera di Microsoft s.r.l.; 3. interessamento anche di server italiani al fine dell'erogazione complessiva del relativo servizio di posta elettronica; 4. ruolo essenziale della attività di marketing sul territorio italiano posta in*

risposta di Yahoo! Inc. all'Ordine del giudice americano di trasmettere quanto richiesto, nella quale si dava atto che "at this time, Yahoo! has no information pertaining to the User ID jpxcnq @yahoo.com, specified in the Court Order" (traduzione dall'inglese: "Ad oggi, Yahoo! non ha informazioni relative all'USER ID jpxcnq @yahoo.com così come indicato nel Court Order" – Ordine del Giudice).

[39] Proprio in relazione all'importanza del problema relativo alla applicabilità ai gestori americani delle norme europee in materia di data retention, **lo stesso Consiglio d'Europa ha chiesto alla procura di Milano di elaborare una posizione giuridica da sottoporre all'attenzione dei partecipanti alla annuale Conferenza Octopus Interface (tenutasi a Strasburgo, 11 marzo 2009**) volta a verificare lo stato di attuazione della Convenzione sul Cybercrime all'interno degli Stati Membri: cfr. gli atti della Conferenza (in particolare la sessione finale significativamente intitolata "Meeting future challenges") reperibili su Internet all'indirizzo *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/IF_2009_presentations/default_en.asp.*

essere da Microsoft s.r.l. – società interamente controllata da Microsoft Corp. – al fine della diffusione del servizio di posta elettronica @hotmail.it).

*Peraltro tale risposta, oltre ad ignorare il mutato lo scenario internazionale negli "accordi tra lo Stato italiano e .. gli U.S.A." alla luce degli effetti della ratifica della Convenzione di Budapest avvenuta con Legge 18 marzo 2008 n. 48[40], non tiene neppure conto – sotto il profilo temporale rilevante per l'imputabilità del comportamento da sanzionare – del fatto che i dati messi a disposizione da Microsoft sono quelli di cui alla risposta del **25 luglio 2008**, come emerge proprio "dagli atti del procedimento per l'accertamento del reato"[41] nonché dell'evidenza che la contestata policy aziendale, volta a limitare ai 60 giorni il periodo di data retention, è stata confermata ancora esistente, nelle note pervenute da Microsoft[42], alla data del **23 ottobre 2008**[43].*

In data 22 maggio 2011 il giudice per le indagini preliminari disponeva l'archiviazione del procedimento, con questa motivazione:

II) La valutazione del compendio probatorio prodotto dal Pubblico Ministero.

La istanza di archiviazione formulata dal Pubblico Ministero deve essere accolta, in quanto non è stato possibile stabilire con elevato grado di credibilità razione l'autore delle condotte criminose per cui si procede.
Le indagini integrative disposte hanno, infatti, dimostrato la obiettiva impossibilità di verificare le dichiarazioni rese da F.F., precludendone in radice la conferma o la confutazione.
La insuperabile incertezza sulla fondatezza delle versione difensiva resa dal F. impone, pertanto, l'archiviazione non essendo plausibile che si possa addivenire in un futuro giudizio di merito ad una affermazione di responsabilità del medesimo *oltre ogni ragionevole dubbio*.

Le indagini suppletiva hanno, peraltro, ulteriormente evidenziato come tale lacuna investigativa non sia superabile per effetto delle disposizioni adottate dal Garante per la Privacy in ordine alla conservazione dell'IP di destinazione.
I dinieghi opposti dai gestori H3G e Microsoft ai decreti di acquisizione degli indirizzi IP di destinazione formulati dalla Pubblica Accusa non hanno consentito di completare il *tracing* ovvero il percorso

[40] Gli Stati Uniti d'America già da tempo avevano ratificato la Convenzione di Budapest, che prevede due precisi obblighi di collaborazione "in tempo reale" (art. 33 in materia di raccolta dei dati del traffico; art. 34 in materia di intercettazione dei contenuti): e dunque, dal momento che anche l'Italia finalmente ha ratificato tale Convenzione, tali obblighi oggi acquistano una loro effettiva valenza giuridica bilaterale (*pacta sunt servanda*).

[41] Cfr. pp. 7– 8: "In merito agli esiti degli accertamenti richiesti alla Microsoft Corporation, tramite la Microsoft srl, relativi agli accessi all'indirizzo di posta elettronica **comicispaventati@hotmail.it** (si rimanda all'**ALLEGATO 7**) è opportuno precisare che:

- In data 26/06/2008, la società Microsoft rispondeva in posta elettronica che: "… l'account risulta non essere più attivo e quindi non risultano più i dati riferiti agli accessi effettuati dal suddetto account ne tantomeno i dati di registrazione. …".
- Nella stessa risposta Microsoft precisava inoltre che: "… il database di Microsoft Corporation conserva i dati per un massimo di 60 giorni (cd. **data retention** – ndr), dopo di che vengono cancellati; inoltre se l'account hotmail non viene utilizzato entro 90 giorni questo viene automaticamente disattivato."

Poiché dagli accertamenti tecnici effettuati dagli scriventi in data 20/06/2008 è emerso che, contrariamente a quanto comunicatoci precedentemente dalla società Microsoft, l'indirizzo di posta elettronica **comicispaventati@hotmail.it** era ancora attivo, il giorno 24/07/2008, presso l'ufficio del P.M. […] veniva sentita a sommarie informazioni […]

Il giorno successivo (25/07/2008), a parziale scioglimento delle riserve, […] con una email forniva i dati relativi al predetto indirizzo di posta elettronica precisando che la prima riposta con esito negativo era dovuta ad un banale errore di trascrizione. I dati forniti comprendevano, oltre agli IP di creazione dell'account, anche i Log di connessione, **relativi agli ultimi 60 gg** da tale (successiva) elaborazione.

Sulla base dei dati forniti emergeva che nell'arco di tempo compreso tra l'invio del primo e del secondo commento vi era stato un accesso alla casella di posta elettronica e l'IP di connessione era lo stesso dell'invio dei post (62.13.173.176). Per questo motivo si ritiene plausibile che l'autore degli accessi sia lo stesso dell'invio dei commenti".

[42] Cfr. pp. 13;15.

[43] Cfr. nota di […], responsabile dell'Ufficio Affari Legali di Microsoft s.r.l., in atti (nonché inviata al Ministero dello Sviluppo Economico insieme all'intero incartamento procedimentale).

investigativo a ritroso inteso ad acclarare l'autore della condotta criminosa perpetrata mediante strumenti informatici.

Tali dinieghi, tuttavia, si rivelano assolutamente ingiustificati e, come hanno evidenziato le indagini, traggono origine dai provvedimenti sanzionatori adottati dal Garante per la Protezione dei Dati Personali nelle *"Prescrizioni sulla conservazione dei dati di traffico"*, che assimilando l'indirizzo IP di destinazione al contenuto stesso della comunicazione, ne hanno imposto la immediata cancellazione.

Tali prescrizioni si rivelano, tuttavia, *illegittime per violazione di legge* e *per difetto di competenza*.

La Corte Costituzionale ha reiteratamente affermato (v. sentenza n. 34 del 1973), che nell'art. 15 della Costituzione *"trovano protezione due distinti interessi: quello inerente alla libertà e alla segretezza delle comunicazioni, riconosciuto come connaturale ai diritti della personalità definiti inviolabili dall'art. 2 della Costituzione, e quello connesso all'esigenza di prevenire e reprimere i reati, vale a dire ad un bene anch'esso oggetto di protezione costituzionale"* (v. anche sentt. nn. 120 del 1975, 98 del 1976, 223 del 1987, 366 del 1991).
Pertanto, l'inderogabile dovere di prevenire e di reprimere i reati deve essere svolto nel più assoluto rispetto di particolari cautele dirette a tutelare un bene, l'inviolabilità della segretezza e della libertà delle comunicazioni, strettamente connesso alla protezione del nucleo essenziale della dignità umana e al pieno sviluppo della personalità nelle formazioni sociali (art. 2 della Costituzione).

Il bilanciamento di interessi tra la libertà e la segretezza delle comunicazioni informatiche e l'interesse statuale all'accertamento della prevenzione e della repressione dei reati imposto dalla Carta Costituzionale è, tuttavia, indebitamente obliterato dalle prescrizioni del Garante che, accordando prevalenza esclusivamente alla *privacy* informatica, pregiudicano irrimediabilmente l'interesse alla persecuzione dei reati senza operare alcuna forma di contemperamento, costituzionalmente imposto (C. Cost. n.281/1998 e n.81/1993), tra i medesimi.

D'altra parte tale bilanciamento di interessi costituzionalmente rilevanti è rimesso dall'art. 15 Cost. al legislatore e non già ad una autorità amministrativa, per quanto connotata da particolari requisiti di indipendenza.

Del resto, secondo una consolidata ermeneusi dottrinale e giurisprudenziale, l'art. 15 della Costituzione enuncia una riserva assoluta di legge e, pertanto, la potestà regolamentare in tale ambito può esplicarsi esclusivamente nelle forme del regolamento esecutivo.

Ne consegue che le statuizioni del Garante per la Protezione dei dati Personali non possono delineare nel perimetro della categoria dei dati relativi al traffico telematico, *in assenza di adeguato fondamento legale*, una disciplina dell'indirizzo IP difforme da quella prevista dal legislatore comunitario e nazionale e, segnatamente, prevedere un termine inferiore di *data retention* rispetto a quello imposto dal legislatore comunitario e nazionale o, addirittura, la sua immediata cancellazione.

D'altra parte, il Pubblico Ministero nell'esercizio dell'attività di repressione dei reati, costituzionalmente doverosa ai sensi dell'art. 112 Cost., non può osservare altri limiti che quelli imposti dalla legge (e non già quelli dettati dalla autorità amministrativa).

L'indirizzo IP di destinazione non può, inoltre, essere considerato coincidente di fatto con *"il contenuto della comunicazione"* e, pertanto, non può essere escluso dal regime normativo comunitario e nazionale sopra delineato.

L'indirizzo IP di destinazione è un dato identificativo esterno al contenuto della comunicazione e, più precisamente, un (semplice) numero di telefono relativo alla richiesta connessione, dal quale –per ovvi motivi– non è possibile automaticamente risalire all'identità dell'effettivo utilizzatore del *computer*.

In altri termini, l'indirizzo di IP non è altro che un numero che identifica univocamente nell'ambito di una singola rete i dispositivi collegati con una rete informatica, prescindendo dal contenuto della comunicazione.

D'altra parte, l'art. 5, paragrafo 2, della direttiva 2006/24/CE espressamente contrappone *"i dati relativi al traffico, i dati relativi alla ubicazione delle persone sia fisiche che giuridiche ed i dati connessi necessari per identificare l'abbonato o l'utente registrato"* al *"contenuto delle comunicazioni elettroniche"*.

La Corte Costituzionale (C. Cost. n.281/1998 e n.81/1993) e la Corte di Cassazione (*ex plurimis*: Cass., SS.UU., 23.2.2000, n.6, *D'Amuri*, Rv.215841; Cass. 7.1.2010, n. 9416, *Congia ed altri*, Rv.246774), del resto, in numerose pronunce hanno differenziato rigorosamente la disciplina di acquisizione dei dati esterni della comunicazione da quella della captazione del contenuto della comunicazione stessa in ragione *"della diversa forma di intrusione nella sfera della riservatezza"*, senza possibilità alcuna di sovrapposizioni o di indebite equiparazioni *quoad substantiam*.

La interpretazione del Garante per la Protezione dei dati Personali si rivela, inoltre, assolutamente infondata ed illegittima alla stregua della normativa, comunitaria e nazionale, vigente *in subiecta materia*.

Il medesimo bilanciamento di interessi tra la *privacy* e l'interesse statuale all'accertamento della prevenzione e della repressione dei reati è, infatti, riproposto dalla normativa comunitaria di settore.

Infatti, la direttiva 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, impone agli Stati membri di proteggere la riservatezza delle comunicazioni elettroniche e vieta la conservazione dei dati relativi al traffico generati nel corso delle comunicazioni, ad eccezione della conservazione espressamente autorizzata per i fini indicati nella direttiva medesima.
L'art. 15, par. 1, di tale direttiva consente che gli Stati membri possano adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui ai predetti articoli 5 e 6 solo quando tale restrizione costituisca *"una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica"*.
Inoltre, il medesimo principio è riaffermato dal 4) considerando della direttiva 2006/24/CE riguardante la conservazione di dati generali o trattatati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.
Del resto, tale direttiva espressamente persegue *"l'obiettivo di armonizzare le disposizioni degli Stati membri relative agli obblighi, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, relativi alla conservazione di determinati dati da essi generati o trattati, allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi, quali quelli definiti da ciascuno Stato membro nella propria legislazione nazionale"*.
La direttiva 2006/24/CE, inoltre, all'art. 6, nel declinare in ambito comunitario il bilanciamento di interessi tra *privacy* ed interesse statuale alla repressione delle condotte criminose, afferma che *"gli stati membri provvedono affinché le categorie di dati di cui all'articolo 5 siano conservate per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione"*.
Del resto, nella categoria di *"dati da conservare"* delineata dall'art. 5 della medesima direttiva figurano espressamente per l'accesso *Internet* e la posta elettronica *"l'identificativo dell'utente, ...nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati assegnati l'indirizzo di protocollo Internet (IP), un identificativo di utente o un numero telefonico"*.
Parimenti, alla medesima categoria, sono ascritti anche per l'accesso Internet, la posta elettronica via Internet e la telefonia via Internet *"data e ora del log-in e del log-off del servizio di accesso Internet sulla base di un determinato fuso orario, unitamente all'indirizzo IP, dinamico e statico, assegnato dal fornitore di accesso Internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato"*.
Inoltre, sul piano della disciplina normativa nazionale, l'art. 132 del Codice in materia di protezione dei dati personali (D. Lgs. 30.06.2003, n. 196) nella formulazione vigente prevede che *"Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico, sono conservati dal*

fornitore per ventiquattro mesi dalla data di comunicazione, per finalità di accertamento e repressione dei reati…".
Il medesimo articolo sancisce, peraltro, che *"…, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione".*

Del resto, nella sintassi del D.Lgs. 30 maggio 2008, n. 109 *("Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE"*), che ha novellato il Codice in materia di protezione dei dati personali, l'art. 1 precisa che *"si intende:…*

b) per dati relativi al traffico: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione, ivi compresi i dati necessari per identificare l'abbonato o l'utente;
f) per identificativo dell'utente: l'identificativo unico assegnato a una persona al momento dell'abbonamento o dell'iscrizione presso un servizio di accesso internet o un servizio di comunicazione internet;
g) per indirizzo di protocollo internet (IP) univocamente assegnato: indirizzo di protocollo (IP) che consente l'identificazione diretta dell'abbonato o utente che effettua comunicazioni sulla rete pubblica".

Inoltre, l'art. 3 di tale testo normativo precisa che *"le categorie di dati da conservare per le finalità di cui all'articolo 132 del Codice sono le seguenti:*

a) i dati necessari per rintracciare e identificare la fonte di una comunicazione:
…
2) per l'accesso internet:
2.1 nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati univocamente assegnati l'indirizzo di protocollo internet (IP), un identificativo di utente o un numero telefonico;
3) per la posta elettronica:
3.1 indirizzo IP utilizzato e indirizzo di posta elettronica ed eventuale ulteriore identificativo del mittente;
3.2 indirizzo IP e nome a dominio pienamente qualificato del mail exchanger host, nel caso della tecnologia SMTP ovvero di qualsiasi tipologia di host relativo ad una diversa tecnologia utilizzata per la trasmissione della comunicazione;
…
2) per la posta elettronica:
2.1 indirizzo di posta elettronica, ed eventuale ulteriore identificativo, del destinatario della comunicazione;
2.2 indirizzo IP e nome a dominio pienamente qualificato del mail exchanger host (nel caso della tecnologia SMTP), ovvero di qualsiasi tipologia di host (relativamente ad una diversa tecnologia utilizzata), che ha provveduto alla consegna del messaggio;
2.3 indirizzo IP utilizzato per la ricezione ovvero la consultazione dei messaggi di posta elettronica da parte del destinatario indipendentemente dalla tecnologia o dal protocollo utilizzato;
3) telefonia, invio di fax, sms e mms via internet:
3.1 indirizzo IP, numero telefonico ed eventuale altro identificativo dell'utente chiamato;
3.2 dati anagrafici dell'utente registrato che ha ricevuto la comunicazione;
3.3 numero o numeri a cui la chiamata è trasmessa, nei casi di servizi supplementari come l'inoltro o il trasferimento di chiamata;
c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione:
1) per la telefonia di rete fissa e la telefonia mobile, data e ora dell'inizio e della fine della comunicazione;
2) per l'accesso internet:
2.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di accesso internet, unitamente all'indirizzo IP, dinamico o statico, univocamente assegnato dal fornitore di accesso internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato;
3) per la posta elettronica:

3.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di posta elettronica su internet ed indirizzo IP utilizzato, indipendentemente dalla tecnologia e dal protocollo impiegato;
4) per la telefonia, invio di fax, sms e mms via internet:
4.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio utilizzato su internet ed indirizzo IP impiegato, indipendentemente dalla tecnologia e dal protocollo usato;
…";
In tale contesto normativo *"i dati relativi al traffico telematico",* ai quali va ascritto per espressa previsione del legislatore l'indirizzo IP di destinazione, devono, pertanto, essere *"conservati dal fornitore per dodici mesi dalla data della comunicazione"* ai sensi dell'art. 132 del Codice in materia di protezione dei dati personali.
D'altra parte, come già ricordato, anche la direttiva 2006/24/CE prevede all'art. 6 che *"gli Stati membri provvedano affinché le categorie di dati di cui all'art. 5* [tra i quali è espressamente contemplato l'indirizzo IP] *siano conservate per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione"*.

D'altra parte, il D.Lgs. 30 maggio 2008, n. 109 impone specificamente ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che offrono servizi di accesso a *Internet* (*Internet Access Provider*) di assicurare la disponibilità e l'effettiva univocità degli indirizzi di protocollo *Internet* per il lasso di tempo previsto dalla normativa interna.

Infatti, l'art. 162-*bis* (*Sanzioni in materia di conservazione dei dati di traffico*) del Codice in materia di protezione dei dati personali sanziona in via amministrativa*"l'omessa o l'incompleta conservazione dei dati ai sensi dell'articolo 132, commi 1 e 1-bis, del Codice"* e *"l'assegnazione di indirizzo IP che non consente l'identificazione univoca dell'utente o abbonato"*;

Pertanto, le prescrizioni sanzionatorie del Garante per la Protezione dei Dati Personali che impongono la cancellazione dell'indirizzo IP di destinazione sono illegittime e si pongono in insanabile contrasto con la normativa comunitaria e nazionale vigente.

Tali prescrizioni devono, pertanto, essere dichiarate dal giudice penale *incidenter tantum* illegittime per incompetenza e violazione di legge e, di conseguenza, devono essere disapplicate in virtù del contenuto precettivo dell'art. 5 L.20.3.1865, all. E che sancisce che *"In questo, come in ogni altro caso, le autorità giudiziarie applicheranno gli atti amministrativi ed i regolamenti generali e locali in quanto siano conformi alle leggi"*.

Anche tale possibilità, tuttavia, non impedisce il pregiudizio irreparabile alle investigazioni cagionato dalla immediata cancellazione e, pertanto, dalla mancata conservazione per fini di giustizia dell'indirizzo IP di destinazione.

La disapplicazione, infatti, non può che essere operata dal Giudice e non già dall'autorità inquirente ed interviene *in via postuma* esclusivamente nell'ambito di una controversia nella quale venga in rilievo l'applicazione del provvedimento amministrativo.

Se, pertanto, il giudice non può esimersi dal constatare la difformità delle prescrizioni dalla legge, tale intervento non può consentire il recupero del dato informatico ormai irrimediabilmente disperso.

La richiesta di archiviazione deve, pertanto, essere accolta in quanto all'esito delle investigazione non è stato possibile addivenire, con adeguato grado di plausibilità razionale, alla identificazione dell'autore delle condotte criminose per le quali pende il procedimento penale.

Nuovamente "chiamato in causa" anche dai media, la risposta dell'ufficio del garante per la protezione dei dati personali non si è fatta attendere:

> *In riferimento all'articolo «Minacciò il Cavaliere, la privacy lo protegge» (Corriere, 24 maggio) è opportuno fare alcune precisazioni. Nel riportare la decisione di archiviazione del gip di Milano su un caso relativo ad un messaggio «postato» nel 2008 su un blog, si cita un provvedimento del Garante della privacy che avrebbe impedito di risalire all'autore del messaggio. Tale provvedimento, adottato nei confronti di un fornitore di servizi telematici, non si riferiva però al caso in esame. Esso riguardava più in generale il fatto che – in base alla normativa italiana ed europea – al provider è consentito conservare, anche a fini di giustizia, solo i dati di traffico telematico relativi all'accesso alla rete, alla mail e al voip (telefonia internet). La conservazione da parte di un provider dei dati relativi alla navigazione dell'utente (indirizzi Ip o url visitati) non è invece prevista da alcuna normativa italiana ed europea. Laddove essa venisse realizzata implicherebbe il controllo da parte del provider dell'attività sulla rete di tutti i propri utenti, controllo effettuabile solo a seguito di un decreto dell'autorità giudiziaria che disponga un'intercettazione telematica nei confronti di uno o più utenti determinati. In questo quadro, il provvedimento del Garante si è limitato a ribadire, alla luce della normativa europea e nazionale, l'illiceità della conservazione di questi dati da parte del provider. Alla luce di tutto questo, non si può dunque sostenere, come riportato nell'articolo, che il provvedimento del Garante sia stato adottato in difformità con la legislazione vigente, e meno che mai abbia avuto come effetto quello di impedire di fatto un'attività giudiziaria altrimenti possibile*[44].

A noi invece sembra di aver fornito, a chi ha avuto la pazienza di seguirci fino a qui, tutte le informazioni utili affinché possa trarre le proprie considerazioni finali sulla vicenda.

[44] Baldo Meo, Capo ufficio stampa del Garante per la protezione dei dati personali, in *Corriere della Sera*, Interventi & Repliche, 26 maggio 2011, p. 51. Si riporta di seguito il commento del giornalista: "Sul primo punto, era chiaro l'articolo: le prescrizioni del Garante (alle quali le società si erano adeguate) erano del gennaio 2008, per definizione precedenti alla vicenda del 9 giugno 2008. Sul secondo punto, e cioè sul fatto che «non si può sostenere» che «il provvedimento del Garante sia stato adottato in difformità con la legislazione vigente, e meno che mai abbia avuto come effetto quello di impedire di fatto un'attività giudiziaria altrimenti possibile», a sostenerlo non è l'articolo che ho scritto, ma la sentenza di archiviazione che ho citato: «Le prescrizioni sanzionatorie del Garante che impongono la cancellazione dell'indirizzo Ip di destinazione – scrive il giudice Fabrizio D' Arcangelo – sono illegittime e si pongono in insanabile contrasto con la normativa comunitaria e nazionale vigente. Devono, pertanto, essere dichiarate dal giudice penale illegittime per incompetenza e violazione di legge e, di conseguenza, disapplicate», il che «tuttavia non impedisce il pregiudizio irreparabile cagionato alle investigazioni».