Archivio Penale
settembre–dicembre 2013 fascicolo 3 anno LXV
ISBN 978-88-548-6177-0
DOI 10.4399/97888548617708
pag. 865–878

Cloud Forensics e nuove frontiere delle indagini informatiche nel processo penale

Stefano Aterno, Marco Mattiucci

1. Definizione teorica ed implementazioni reali dei *Cloud systems*. Una grande quantità di indagini di polizia giudiziaria si è spostata su Internet ed in particolare sui sistemi *Cloud* a causa della vasta diffusione di supporti di memoria virtuali come ad esempio *dropbox, google drive*, o per l'estrema diffusione di *social network* come *Facebook* che ricreano interi ambiti virtuali in cui condividere informazioni, idee, servizi, interessi e comunicazioni.

Un *cloud computing* è un sistema di elaborazione distribuito, basato su Internet. Più chiaramente, può essere paragonato ad un grande e sofisticato *personal computer* (sistema di elaborazione) non realizzato da un sistema elettronico fisicamente individuabile in un luogo ma da un insieme di sistemi elettronici connessi tra loro mediante la Rete Internet e quindi mediante una connessione telematica. In tal modo, Internet — da mezzo di comunicazione — diviene mezzo costitutivo di diverse "nuvole" (*cloud*) di sistemi federati che realizzano servizi per i loro utenti. Il motore di ricerca Google è un esempio di *Cloud*; l'utente lo usa attraverso una semplice pagina *web* ma non è possibile stabilire con certezza "chi" risponde alle domande che l'utente pone durante la ricerca e "dove" esso sia.

La risposta al "chi" ed al "dove" è terribilmente condizionata. Il *Cloud* di Google (ed in genere ogni *Cloud*) è un sistema altamente dinamico ed autoriconfigurabile, in grado di far fronte alla richiesta di servizi a seconda delle sue disponibilità di risorse. Se ad esempio il *server* di Google (fornitore di servizi) che risponde alla nostra domanda (richiesta di servizio) fosse troppo occupato e non rispondesse in quel momento, un altro, appartenente alla stessa "nuvola", prenderebbe prontamente il suo posto e l'utente non vedrebbe il minimo ammanco di servizio. Questa incertezza di "chi" e "dove" alla base del *Cloud* ne fa un argomento fortemente dibattuto nell'ambito della *forensics* in ambito *Cloud*.

Il *Cloud Forensics*, ossia la branca del *Digital Forensics* dedita ad indagini ed accertamenti tecnici su *Cloud*, soffre fortemente la mancanza di territorialità ed identificabilità tipici delle "nuvole" di Internet. Ma, d'altro canto, l'avvento dei sistemi *Cloud* è inevitabile. Ci sono diverse ragioni che dettano l'ineluttabilità dei sistemi *Cloud* su Internet (la loro crescita negli ultimi anni

è incalcolabile ed il *trend* continua in tale direzione[1]) ed è bene tenerne conto per capire come le indagini di polizia giudiziaria ne saranno sempre più influenzate: integrazione con i cellulari[2], diminuzione dei costi[3], memorie infinite[4], servizi illimitati[5], aterritorialità ed anonimato[6]. Il che porta a pensare che nell'arco di poche decine di anni Internet si trasformerà in *Intercloud*, una federazione di "nuvole" basate su servizi e dati che potranno essere accedute dall'utente in maniera semplice ed efficace dismettendo gli ormai vecchi concetti di indirizzi internet (URL) ed IP (*Internet Protocol Address*) continuamente usati nelle indagini odierne.

I sistemi di *Cloud Computing* si sono affermati a seguito di due conquiste tecnologiche fondamentali della nostra società: la virtualizzazione e la remotizzazione. Quanto alla prima, esistono programmi del pari di *Parallels, VMware, VirtualBox*, ecc., il cui scopo è consentire di eseguire come programmi al loro interno interi sistemi operativi e quindi di fatto realizzare delle "macchine virtuali" ossia computer che "vivono" all'interno di

1. In argomento, per maggiori approfondimenti, si preferisce rinviare a Lilllard, Garrison, Schiller, Steele, *Digital Forensics for Network, Internet and Cloud Computing*, Elsevier, 2010, p. 39; Peterson, Shenoi, *Advances in Digital Forensics IX*, in Atti de *IX IFIP WG 11.9, International Conference on Digital Forensics*, Orlando, FL, USA, 28–20 gennaio 2013.

2. Impiegare i servizi di un C*loud* su *smartphone* (cellulari di ultima generazione) è semplice ed incredibilmente efficace. Basti pensare al fatto che *Facebook* è ormai integrato nativamente in qualsiasi cellulare ed il difficile è divenuto "spegnerlo" e non usarlo. Si può riflettere sui servizi di Google (*Android*) o *iCloud (Apple*) in cui magicamente tutto ciò che è sul proprio PC o Mac di casa/ufficio si ritrova tranquillamente sullo *smartphone* in treno, il proprio *backup* dei dati ed delle agende vengono salvati su una nuvola "astratta" e quindi non preoccupa più perdere chiavette USB o *hard disk*/cellulari, ecc. L'utente si svincola con semplicità dagli oggetti materiali ed il *Cloud* favorisce la mobilità dei dispositivi e dei dati nell'intero *cyber*–spazio.

3. I servizi *Cloud* costano assolutamente meno di qualsiasi servizio equipollente auto–costruito ed auto–gestito. Si terziarizzano infatti le manutenzioni, gli acquisti ed inoltre si paga solo per l'uso reale e non per il possesso. Il *pay–per–use* è proprio il punto chiave che ha lanciato e sostiene oggi il mondo *Cloud*.

4. Non si dice niente di nuovo se si afferma che i moderni sistemi di elaborazione, dai computer ai cellulari, richiedono quantità di memoria digitale sempre più alte e la tendenza inevitabile è a delocalizzarle, cioè spostarle su un sistema C*loud* virtualizzandole e rendendole potenzialmente infinite ad un costo irrisorio. Basti pensare alla *Google mail* meglio conosciuta come *gmail*, una potente implementazione di *Cloud* sui servizi di posta elettronica. Essa risulta priva di costi per l'utente e lo spazio di archiviazione per gli allegati e la posta cresce di anno in anno rendendo praticamente inutile la cancellazione dei dati da parte dell'utente (lo stesso *Google* consiglia di evitare la cancellazione in quanto lo spazio sarà potenzialmente tale da contenere qualsiasi tipo di attività umana per anni).

5. Su *Cloud* qualsiasi tipo di servizio informatico o telematico è ricostruibile e gestibile direttamente dal *browser* (*Explorer, Safari, Firefox, Chrome*, ecc.). Si può implementare dalla sicurezza di canali criptati (servizi di comunicazione) al *VoIP* (*voice over* IP, ovvero telefono *online*), *Chat, Video*, filmati in s*treaming*, fino ad interi sistemi di elaborazione ed addirittura reti di calcolatori. Non ci sono limitazioni: potenzialmente il limite è solo nella fantasia umana.

6. Purtroppo (nota dolente per le indagini) i sistemi *Cloud* sono una delle migliori garanzie per realizzare l'anonimato e per emanciparsi da "antichi" ed "angusti" confini territoriali e nazionali. Da ciò la possibilità di operare al di fuori delle leggi ed al di fuori della fiscalità (punto quest'ultimo che già ha toccato *Google* ed *Amazon*, due tra i maggiori *Cloud* della terra che in diverse nazioni hanno avuto questioni con il fisco per accertamenti fiscali e per imposte sul valore aggiunto non pagate).

altri *computer*. Con questa modalità, ad esempio è possibile avere un PC *Windows* che opera dentro un *Apple Mac*. L'*hardware* è unico, quello del *Mac*, ma l'utente può lavorare simultaneamente con due computer diversi condividendo tastiere, *hard disk*, *monitor*, ecc. Il processo di virtualizzazione è ad oggi talmente spinto che dentro un computer è possibile simulare diversi computer virtuali collegati tra loro in rete; in pratica è possibile avere delle intere reti virtuali solo in un computer di casa. Quanto alla seconda conquista (la remotizzazione), ci sono programmi come *LogMeIn*, *SplashTop*, ecc., che permettono ad esempio di accedere dal cellulare o dal PC d'ufficio al computer di casa (accesso e connesso ad Internet ovviamente). Si può quindi agire sul computer di casa come se si fosse lì mentre in realtà ci si trova a distanze chilometriche. La remotizzazione è anch'essa talmente spinta che è divenuta una costante in qualsiasi sistema di gestione della manutenzione delle reti (l'utente viene invitato ad alzare le mani dalla tastiera e l'amministratore prende possesso della sua macchina a distanza facendo vedere all'utente cosa fare, scrivendo sullo schermo, muovendo il *mouse*, ecc.).

La virtualizzazione ha trovato supporto nella vasta disponibilità di microprocessori *multicore* già predisposti in tal senso (essi hanno un *hardware* che gestisce la virtualizzazione ad alta velocità) ed impiegati in qualsiasi computer anche di piccola taglia. La remotizzazione ha beneficiato dell'incremento di velocità di trasmissione su Internet (ampiezza di banda), elemento che gli utenti chiedono costantemente ai *provider* di servizi telefonici.

1.1. Struttura e tipi di servizi *Cloud*. Rifacendosi a quanto sopra indicato, un sistema *Cloud* è una federazione di sistemi virtualizzati e remotizzati su Internet in quantità dipendente dal tipo di servizio che devono fornire (struttura dinamica *on–demand*). Come tale si possono individuare:

a) *Cloud Client*: *PC, Smartphone, Embedded System* (es. *iPad*), ecc. su cui è presente almeno un sistema operativo (es. Windows, MacOS, ecc.) ed un *software* di *browsing* su Internet (Explorer, Safari, Firefox, Chrome, ecc.). Il *Cloud Client* è il sistema che l'utente impiega per chiedere servizi al *Cloud* e riceverne risposte. Il maggiore artefice di questo è ovviamente il *browser* impiegato e l'indipendenza dal sistema operativo è quasi sempre garantita.
b) *Cloud Service Provider (CSP):* equivalente al ISP (*Internet Service Provider*) il CSP è la ditta che supporta e gestisce il *Cloud* in questione regolando le erogazioni di servizi e le utenze.
c) *Cloud per servizi software (SaaS)*: *Software as a Service* (SaaS), è l'acronimo di un servizio *Cloud* che è caratterizzato per rendere disponibile all'utente dei *software* pagandoli solo in base all'impiego o non pagandoli affatto. Sparisce quindi il concetto di licenza del *software* per

lasciare il posto a quello di software *pay–per–use* con evidenti risparmi ma soprattutto con la scomparsa necessità di aggiornarlo dato che si impiega online sempre in ultima versione (il *software* come servizio NON si installa sul cliente). Tipici esempi sono gli applicativi *online* che permettono di accedere ai *Google Documents*, in tutto simili agli strumenti del pacchetto *Office* e spesso ad esso compatibili.

a) *Cloud per piattaforma (PaaS): Platform as a Service* (PaaS) identifica un tipo di servizio *Cloud* in cui la nuvola rende disponibili singoli elaboratori remoti completamente virtualizzati. La loro struttura *hardware* risulta addirittura modificabile online ed "a caldo". Si può ad esempio scegliere di impiegare per soli 10 minuti un *personal computer* con un microprocessore *multicore*, diversi *GygaByte* di RAM ed almeno 1 *TeraByte* di *hard disk* per poi distruggerlo immediatamente oppure trasformarlo in un sistema più potente con 16 microprocessori e diversi *TeraByte* di *hard disk*. Il tutto online e con semplici click del mouse, nessun sistema fisico effettivamente viene costruito ed inoltre non è noto in quale parte del mondo la macchina virtuale richiesta operi.
b) *Cloud per Infrastruttura (IaaS): Infrastructure as a Service* (IaaS) è un tipo di servizio *Cloud* in cui si virtualizzano intere reti di computer con *server*, *client* e collegamenti anche di natura diversa. Questo servizio risulta incredibilmente efficiente se ad affittarlo è una ditta in quanto i suoi dipendenti potrebbero iniziare a lavorare e condividere dati e software tra loro immediatamente dopo essersi connessi ad Internet e non ci sarebbero tempi morti di gestione della rete interna o di manutenzione del sistema. Inoltre, qualora la ditta si trasferisca in altra sede o altri uffici, la sua rete interna si trasferirebbe con lei a costi praticamente irrisori.
c) *Cloud per comunicazioni (CaaS): Communication as a Service* (CaaS) sono servizi *Cloud* per la comunicazione digitale. Si pensi ai sistemi di supporto al social *networking*, nessun miglior esempio di questo è possibile. *Facebook* è contemporaneamente un sistema di comunicazione multiutente, un archivio, una *chat*, ecc. per cui integra una grande varietà di servizi di comunicazione *Cloud*.
d) *Cloud per memorie di massa (Remote Virtual Drive)*: i già citati *Dropbox e GDrive* o *Amazon S3* sono i grandi *hard disk Cloud* di *Internet*. Essi permettono di memorizzare un'enormità di dati sulle rispettive nuvole realizzando di fatto drive virtuali accessibili da remoto da una moltitudine di dispositivi diversi (*iPhone, iPad, Tablet*, PC, *Mac*, ecc.).
e) *Cloud for Cloud*: ci sono *Cloud* così potenti e ricchi di risorse (Amazon in testa ovviamente) che forniscono come servizio la possibilità di creare e gestire un proprio *Cloud*. Queste possibilità consentono a

chiunque di divenire CSP a richiesta ed ovviamente pagare in base ad un tariffario e secondo accordi prestabiliti.

Tutti i *Cloud Sercive Provider* (di seguito CSP) sono in grado di fornire tutti i servizi appena evidenziati. Questo dipende dal costo delle risorse necessarie ad implementare, sostenere e fornire tali servizi.

Quando durante un'indagine è necessario "affrontare" un sistema *Cloud,* l'investigatore deve innanzitutto capire preliminarmente con quale tipo di *Cloud* sta confrontandosi e poi andare a verificare il particolare servizio (o l'insieme dei servizi) cui è interessato per le finalità dell'indagine. Ciò in quanto possono essere prese diverse decisioni. In precedenza sono state elencate le principali categorie di servizi, qui di seguito si elencano le classi di *Cloud* attualmente esistenti su Internet:

a) *Public Cloud*: realizzati per mettere a disposizione di più utenti possibili i servizi; solitamene sono gestiti da CSP non necessariamente noti.
b) *Community Cloud*: più soggetti, enti o comunità *on line* mettono in comune (remotizzando e virtualizzando) delle risorse tramite Internet realizzando una "nuvola" che eroga servizi soprattutto ai membri della comunità stessa. I membri della comunità sono noti ma nulla vieta che essi operino e creino il *sistema* da nazioni diverse con ordinamenti diversi. Possono ovviamente esistere delle comunità nascoste transnazionali che impiegano il loro *community Cloud* per condividere servizi di ogni tipo, anche illegale.
c) *Private Cloud*: realizzato e gestito da un ente noto che detiene responsabilità e patrocinio dei dati. Spesso questo spazio viene dall'ente spesso affittato a terzi soggetti che hanno bisogno di questo servizio più privato e riservato.
d) *Hybrid Cloud:* per motivi economici è talvolta possibile che si combinino *Cloud* privati (molto costosi) con *Cloud* pubblici o di comunità virtuali. In tal caso funzionamento e struttura dipendono dalla loro struttura.

1.2. Sopralluogo e repertamento sui *Cloud*. Sono possibili ed ovviamente sono attività virtuali. Per sopralluogo virtuale s'intende la "visita" *on–line* di un'area o sistema del *Cloud* per osservarne i servizi (non solo i dati) attivi, le richieste, le forniture, i *log*, ecc. Per repertamento s'intende sostanzialmente la copia di dati e l'acquisizione di evidenze direttamente accedendo al *Cloud* nell'ambito dell'indagine specifica.

Il sopralluogo può essere svolto senza eccessivi problemi tecnici se il CSP collabora (ad esempio si trova in Italia ed ha un'identificazione certa ed

è facilmente raggiungibile dall'autorità giudiziaria procedente; al contrario l'unico modo per effettuare un sopralluogo su *Cloud* all'estero è tramite le intercettazioni telematiche. Purtroppo la maggior parte dei *Cloud* implementa meccanismi di criptazione per operare *online* da cui l'unica possibilità rimane l'intercettazione tramite captatore informatico (*Remote Control System*, da alcuni definito *"trojan"*)[7].

Per il repertamento si devono operare copie di dati in condizioni dinamiche (il *Cloud* non può spegnersi) per cui si è in presenza di un'attività irripetibile. A questo proposito, si stanno sviluppando una serie di nuovi strumenti forensi in grado di procedere a tali acquisizioni.

Senza scendere nei dettagli, al momento questa attività è lasciata alla perizia di tecnici altamente specializzati che devono avere la capacità di regolare le loro scelte tecniche in base alla singola situazione che di volta in volta devono affrontare.

L'acquisizione su *Cloud* attraverso il captatore informatico a cui sopra si è fatto cenno, può risultare strumento essenziale ma verrebbe impiegato al di fuori di quella che è l'attività di intercettazione telematica. Purtroppo o per fortuna, in Italia, in questo ambito, il problema è ancora aperto e si discute sulla liceità o meno della procedura, dell'applicazione delle norme del codice di procedura penale e delle necessarie garanzie.

In un sistema *Cloud* perfetto il *Cloud Client* (es. il cellulare dell'indagato) non memorizzerebbe nessuna evidenza dell'attività svolta ma fortunatamente siamo ancora lontani da tale perfezione per cui l'indagine sul *Client* (sequestro ed analisi forense classica del dispositivo secondo le linee guida della *digital forensics*) ha ancora molto senso. Ci si concentrerà soprattutto sulle tracce che riconducono ad attività del *Browser* per identificare il *Cloud*, i collegamenti impiegati, le comunicazioni in chiaro svolte, ecc.

Successivamente si procede verso il *Cloud* e qui la sua classe diviene determinante. Per *Cloud* privati si procede direttamente verso il CSP che è individuabile legalmente: se è in Italia si passa ad una indagine classica su Internet e si chiede al CSP di collaborare su indicazione del p.m.; se non è in Italia si devono cercare altri strumenti tra cui la collaborazione investigativa (es. il CSP ha supportato con i suoi servizi *Cloud* altri reati in altri stati per cui potrebbe già essere sotto indagine) e/o la rogatoria internazionale che purtroppo soffre dei suoi limiti temporali (i *Cloud* si ridefiniscono in secondi e minuti mentre la rogatoria è uno strumento che impiega tempi dell'ordine di mesi). Per *Cloud* pubblici il discorso si complica, data la vastità del numero di utenti che in genere servono e le garanzie minime per il servizio (dato che spesso ha costi irrisori se non nulli) le tracce di attività al suo interno sono di

7. Per una prima analisi del fenomeno del captatore informatico anche alla luce di una sentenza italiana, Cass., Sez. V, 14 ottobre 2009, Virruso ed altri, in *Mass. Uff.*, n. 246954, sia consentito rinviare a Aterno, Cajani, Costabile, Mattiucci, Mazzaraco, *Manuale di Computer Forensics*, Forlì, 2012; ed inoltre, Aterno, voce *Digital Forensics*, in *Dig. Pen.*, Agg., Padova, p. 58, in corso di pubblicazione.

principio scarse se non inesistenti, inoltre il CSP non è sempre individuabile nonché talvolta risponde asserendo che non ha nella sua disponibilità i dati di cui al servizio indagato. Questo può succedere tecnicamente ed un semplice esempio chiarifica il problema. Su alcuni servizi di *Remote Virtual Drive* pregiati come *iCloud* di Apple è impossibile memorizzare dati criptati che siano facilmente identificabili come tali. Questo perché Apple si riserva di proteggere i dati fino a quando l'A.G. degli USA non gli chiede di fornirli. Se un utente memorizza su *Cloud* un *file* criptato con un suo metodo ed algoritmo quando la p.g. gli chiederà tale *file* il CSP lo fornirà com'è e quindi chiuso dal cripto per cui inutile (non leggibile dalla p.g.). I *Cloud* pubblici vengono impiegati per servizi molto più articolati di un semplice *storage* di *file* e nella maggior parte dei casi la criptazione è uno strumento che mette in campo l'utente e non il *Cloud* per cui il CSP si arrende a ciò dicendo che non è responsabile di quello che accade tramite la sua "nuvola" perché non può vederlo o valutarlo.

Per i *Community Cloud* il fenomeno della loro espansione su Internet è enorme e se ne possono trovare di ogni tipo, sia di natura lecita che illecita. Il fatto che i singoli componenti della community che costituiscono il *Cloud* possano essere in posti diversi della terra è determinante in quanto i dati contenuti nel *Cloud* non necessariamente devono risiedere in un posto preciso ed il *Cloud* li può redistribuire in giro per il mondo. Un esempio semplificato rende immediatamente l'idea della problematica. Si consideri un documento *Word* di diversi MB con al suo interno testo, foto, riferimenti, tabelle, ecc., che costituisca evidenza di reato in Italia e si supponga di memorizzare tale documento in un *Community Cloud* in cui i meccanismi di memorizzazione criptano e spezzettano il documento in diverse parti memorizzandole in diverse zone della terra. Ognuno dei pezzi, separatamente dagli altri, non ha senso compiuto e non può essere decrittato, per cui non è evidenza di reato nemmeno in Italia. La domanda che ne consegue è: dov'è il documento? E quale legge si può ad esso applicare? Il documento è realmente sparso tra più nazioni. Se si accede al *Cloud* lo si può vedere per intero ma se lo si copia dai server che formano il *Cloud* nulla si ottiene. Il repertamento vecchio stile come copia di dati non è più utile. Per assurdo se si copia il *monitor* mentre l'utente accede al documento virtuale si ha l'unica evidenza possibile della sua esistenza e questo riporta ovviamente all'uso di mezzi altamente intrusivi per le indagini come i *trojan* ed i *Remote Control System* che tra le funzioni hanno l'acquisizione a distanza delle immagini del *monitor*.

2. Quale norme e garanzie in tema di ispezione, perquisizione e sequestro in ambiente *Cloud computing*? Come accennato in precedenza, durante le indagini è possibile rinvenire sistemi informatici o telematici accesi e con operazioni in pieno svolgimento. I casi sono sostanzialmente

di due tipi: il primo è il caso — ormai di scuola — relativo a comunissimi *personal computers* o apparati informatici che si rinvengono accesi sulla scena del crimine ma che sostanzialmente sono facilmente asportabili e quindi nella maggioranza dei casi oggetto di spegnimento, sequestro e successiva acquisizione e analisi forense. La seconda ipotesi è quella in cui le circostanze di fatto e di luogo non consentono di acquisire il contenuto di un sistema informatico attraverso la consegna materiale dei dati o comunque non consentono di sequestrare dati e supporti informatici (*server)* senza provocare un blocco del servizio (spesso) pubblico o di pubblico interesse (si pensi appunto a società che affittano o vendono spazio in sistemi di *Cloud computing*, gestori di comunicazioni accessibili al pubblico, all'ipotesi di operatori di telefonia, *internet service provider*).

Con le modifiche della legge del 18 marzo 2008, n. 48 (legge di ratifica della convenzione di Budapest del 2001) le norme del codice di procedura penale disciplinano la "cristallizzazione della *digital evidence*" e tendono a garantire l'integrità dei dati[8].

Per i sistemi *Cloud* l'osservanza di tale normativa risulta alquanto problematica. Davanti ad un normale supporto informatico, solitamente, si procede attraverso l'osservanza di tecniche di spegnimento del sistema in grado di preservare la memoria *Ram*, fino a soluzioni tecnologicamente avanzate per i casi più complessi e delicati. Nelle ipotesi di intervento in ambito *Cloud* è frequente che gli operatori non conoscano esattamente in quale *server* sono memorizzati i *files* d'interesse e sono di fatto impossibilitati a sequestrare (o anche solo ispezionare) tutto il contenuto di un account su *Cloud computing*. Nella maggior parte dei casi non è neanche pensabile interrompere il servizio soprattutto nei casi in cui si ricerca la prova presso terzi e non direttamente nei sistemi di proprietà dell'indagato.

In tali situazioni affinché l'indagine non si blocchi di fronte a difficoltà di ordine pratico è necessario che l'organo procedente si ponga l'interrogativo su cosa sequestrare. È di tutta evidenza che soprattutto in tali situazioni e di fronte a tali numeri non tutto costituisce corpo del reato e non tutto è opportuno sequestrare o acquisire. Deve effettuarsi una scelta preventiva dei dati che possono essere utili alle indagini e ciò che invece può essere

8. Tonini, *Manuale di procedura penale*, Milano, 2013, p. 357, sul punto, volendo anche Aterno, *Acquisizione e analisi della prova informatica,* in *Dir. pen. proc.*, 2008, 6, suppl. (Dossier: *La prova scientifica nel processo penale*, a cura di Tonini), 61. Cfr. altresì Cuniberti, Gallus, Micozzi, Aterno, *Commento alla legge di ratifica della convenzione di Budapest del 23 novembre 2001*, in *www.giuristitelematici.it*; Luparia, *I profili processuali*, in *Dir. pen. proc.*, 2008, 717 ss.; Marcoccio, *Convention on cybercrime: novità per la conservazione dei dati*, in *www.interlex.it*; Picotti, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, 700; Id., *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Dir. Internet*, 2008, 5, 437 ss.; Resta, *La disciplina acquista maggiore organicità per rispondere alle esigenze applicative*, in *Guida dir.*, 2008, 16, 52; Selvaggi, *Cooperazione giudiziaria veloce ed efficace*, in *Guida dir.*, 2008, 16, 72.

trascurato[9]. Dunque è necessario comprendere con esattezza cosa cercare e con quali modalità acquisire ciò che si desidera al fine di consentire però la ripetibilità dell'operazione garantendo la genuinità degli elementi di prova oppure procedere con le modalità delle attività irripetibili *ex* art. 360 c.p.p. Una volta individuati i *file* o le *directory* da acquisire in quanto utili e necessarie alle indagini occorre farlo garantendo l'integrità del *file* e la non modificabilità. Escludendo l'ipotesi di poter salvare il *file* su un supporto esterno (es. *pen drive*) con il tipico comando "salva con nome" in quanto andrebbe a modificare i cd metadati alterando il *file* e il suo contenuto, è possibile invece effettuare una tipica masterizzazione del *files* o dell'intera "cartella" rimanendo nell'ambito di un'attività ripetibile *ex* art. 359 c.p.p.

La giurisprudenza della Corte di cassazione si è pronunciata sul punto e in un caso di documenti informatici utili alle indagini rinvenuti all'interno di un *personal computer* acceso durante una perquisizione ha stabilito che la masterizzazione del *file* non costituisce attività irripetibile bensì attività ripetibile e che pertanto è formalmente corretta[10]. Con un'altra pronuncia, la Suprema Corte si è confrontata con l'acquisizione di un *file* di posta elettronica su un *server* aziendale di una grande banca italiana in un procedimento che riguardava il furto d'identità, il trattamento illecito di dati personali e alcune presunte truffe ai danni di utenti *e–bay*. Il caso affrontato dai giudici di legittimità riguardava una richiesta di sequestro del pubblico ministero erroneamente fondata sull'art. 254–*bis* c.p.p. (sequestro presso fornitori di servizi informatici, telematici e di telecomunicazioni) in quanto in realtà rivolta ad un istituto bancario che presso i propri *server* conservava il *file delle email* in formato *"pst"* delle cartelle *outlook* di posta elettronica dell'indagato. Il caso è stato oggetto di una precedente pronuncia di merito del Tribunale del Riesame di Roma[11], poi impugnata e a cui è seguita una pronuncia della Suprema Corte[12]. Nelle motivazioni di quest'ultime due sentenze della Cassazione ci sono alcuni aspetti che riguardano l'acquisizione di alcuni documenti informatici che forse potevano essere chiariti e spiegati meglio.

Per esempio, con riferimento alla seconda sentenza citata, quella del *file*

9. Tale scelta può essere effettuata attraverso il ricorso all'ispezione informatica prevista ai sensi dell'art. 244 c.p.p. di cui si dirà più avanti.

10. Cass. Sez. I, 25 febbraio 2009, Dell'Aversano, in *Mass. Uff.*, n. 243495; si veda anche Id., Sez. II, 12 dicembre 2008, Bruno, in *Guida dir.*, 2008, 85, con nota di Cisterna, *Tecniche di ricerca appropriate in base all'attuale quadro normativo*, *ivi*, 2009, 17, 87 ss.

11. Tribunale del Riesame di Roma 8 luglio 2008, Bruno, *inedita*, ma di cui ampi passaggi possono rinvenibili in Aterno, Cajani, Costabile, Mattiucci, Mazzaraco, *Manuale*, cit., p. 488 ss.

12. Cfr. Cass., Sez. II, 13 marzo 2009, Bruno, in *Guida dir.*, 2009, 17, 85. Trattasi della prima sentenza della Suprema Corte dove si fa riferimento a questa tecnica di *hashing* e si nota con favore che negli ultimi tempi, complici alcuni ricorsi in materia di reati informatici, la Corte di Cassazione è stata chiamata a misurarsi con le nuove tecnologie e con il principio relativo di ripetibilità dell'accertamento. Per un commento sul tale sentenza cfr. Cisterna, *Tecniche di ricerca appropriate in base all'attuale quadro normativo*, cit., 87 ss.

di posta elettronica nel server della banca, i giudici di legittimità hanno ritenuto che ogni valutazione di ordine tecnico circa la necessità di effettuare l'*hashing* per poter eventualmente verificare se la copia del *file* nel CD masterizzato sia uguale all'originale (e quindi se il *file* sia stato modificato o meno) è estranea al giudizio di legittimità, sia perché attiene essenzialmente alle modalità esecutive del sequestro sia perché comunque la normativa richiamata dal ricorrente non individua specificatamente le misure tecniche da adottare, limitandosi a richiamare le esigenze da salvaguardare attraverso idonei accorgimenti; la corte ha aggiunto comunque che nel caso di specie, la sezione della polizia postale nell'acquisizione della documentazione informatica relativa all'attività delittuosa oggetto di indagine aveva in concreto adottato le cautele previste dalla legge n. 48 del 2008.

In realtà la suprema Corte in entrambe le sentenze sopra richiamate, non ha tenuto conto che la procedura posta in essere non era affatto idonea a tutelare le finalità indicate dal legislatore negli articoli 247, co. 1–*bis*, e 354, co. 2, del c.p.p. proprio in considerazione della mancata adozione di ciò che stabiliscono questi due ultimi commi citati. Al di là del rilievo fatto dai giudici di legittimità circa il rinvio al dibattimento, sarebbe stato opportuno chiarire meglio ciò che il quest'ultimo giudice deve verificare in concreto in sede di giudizio anche perché non vi è dubbio che già da una lettura delle carte processuali non emergeva alcuna modalità di conservazione del *file* originale sul *server* di posta elettronica della Banca. Se non si adottano le misure tecniche o non si impartiscono le prescrizioni necessarie ad assicurare la conservazione e ad impedire l'alterazione e l'accesso a dati, informazioni e programmi informatici viene violato proprio il dettato normativo ed in particolare un accorgimento di garanzia finalizzato a verificare l'integrità e la conformità all'originale del dato informatico (*file* che contiene tutta la posta elettronica di un dipendente) acquisito da un *server* aziendale (non sequestrato). La riproduzione in copia su un Cd–Rom firmato da tutti gli operanti di polizia giudiziaria e dall'ausiliario di polizia giudiziaria potrebbe non essere sufficiente a assicurare il principio di garanzia ma soprattutto non ha senso se non viene adottato quanto affermato nella seconda parte dell'art. 247 co. 1–*bis* e nella prima parte del comma 2 dell'art. 354 c.p.p. (« *. . . adottare altresì le misure tecniche o impartire le prescrizioni necessarie ad assicurare la conservazione e ad impedire l'alterazione e l'accesso. . .* »)[13].

È di tutta evidenza che non si è tenuto in debito conto che il *file* "originale" di tutta la posta elettronica (es. *outlook*) presente sul *sever*, per sua propria natura e fin tanto che non viene definitivamente tolto da quella sede, è soggetto a continue modifiche anche del tutto involontarie e indipendenti dall'azione del titolare della casella di posta o di soggetti terzi manutentori

13. Per tutti, in generale, si veda, Tonini, *Manuale*, cit., p. 357. Per un approfondimento sul punto specifico sia consentito il rinvio a Aterno, *Acquisizione,* cit., p. 61.

del *server*. Pertanto, senza un "congelamento" o un'asportazione del *file* con un preliminare calcolo di *hash,* (si pensi all'ipotesi di "zippare" il *file* e proteggerlo con *password* lasciandolo anche nel *server* in quanto divenuto cosi immodificabile) si è contravvenuto al disposto dell'art. 247 co. 1–*bis* e al co. 2 dell'art. 354 c.p.p., non consentendo alla difesa, tra le altre cose, di ripetere l'operazione direttamente dal *server* di posta.

Tutta la fase che precede un'acquisizione informatica su *computer* acceso (c.d. *live forensics*) dovrebbe essere debitamente documentata[14].

Esistono anche i c.d. *keylogger* (*software* o *hardware*) in grado di registrare tutto ciò che un utente digita sulla tastiera del *computer* e quindi essere utilizzati all'occorrenza anche per certificare l'autenticità e la genuinità di una operazione di acquisizione fatta dalla polizia giudiziaria durante una *live forensics*. In considerazione dell'alta probabilità di errore nelle acquisizioni informatiche cd *live*, questa tecnica andrebbe suggellata con l'apposizione della firma digitale ai *file* di *log* prodotti dal *software* al fine di certificare l'operato della polizia giudiziaria al di là di quanto potrebbe fare un semplice verbale di polizia dal quale certamente non emergerebbero gli errori inconsapevoli eventualmente commessi. La legge di ratifica della Convenzione di Budapest ha introdotto il concetto di ispezioni informatiche accanto a quello di perquisizioni informatiche (artt. 244 co. 2 e 247 c.p.p.). Alcune brevi riflessioni inducono a ritenere che in realtà una pur minima differenza tra i due strumenti di ricerca della prova può esserci. L'ispezione consiste nel limitare l'operante all'esame obiettivo della situazione di fatto esattamente come essa ricade sotto i sensi percettivi di chi sta procedendo. L'atto ispettivo viene disposto ed effettuato a scopo di percezione visiva personale e di tutto ciò che può essere rilevante per le indagini (art. 244 c.p.p.) con possibilità di eseguire rilievi segnaletici, descrittivi e fotografici ed etimologicamente deriva da "*in–spicio*" ovvero qualcuno guarda "in" qualcosa. Mentre, nella perquisizione, il perquirente "fruga" e l'osservazione visiva è il semplice mezzo per l'attività di ricerca e di apprensione materiale[15]. L'attività ispettiva è per lo più un rilevamento morfologico degli effetti e delle tracce esterne visibili, senza intervento modificatore o invasivo dell'investigatore. Alcune leggi speciali prevedono che la polizia giudiziaria può procedere a "controlli" e "ispezioni" (denominate anche "di sommaria ricerca") che possono "progredire" in vere e proprie perquisizioni quando ciò è necessario in conseguenza di risultati derivanti dall'originario intervento investigativo. In questi casi le ispezioni devono considerarsi atti atipici di indagine e si sostanziano in un'attività di osservazione e percezione che può essere eseguita sia da agenti sia da ufficiali di p.g. e che in via generale può riguardare esclusivamente i

14. Tonini, *Manuale*, cit., p. 357; Aterno, *Acquisizione*, cit., p. 62.

15. Per una compiuta ed esauriente disamina di questi istituti processuali, si veda D'Ambrosio, *La pratica di polizia giudiziaria*, Padova, 2007, II, p. 73.

mezzi di trasporto, i bagagli e gli effetti personali[16]. L'ispezione tende quindi ad assumere informazioni utili attraverso la lettura di segni che abbiano significati ricavabili dall'applicazione di criteri argomentativi: se in un luogo si rinviene della cenere o del fumo ciò fa pensare che vi è stato del fuoco.

Ciò detto, si pone una duplice domanda. Se sia possibile ipotizzare un'attività ispettiva su di un sistema di *Cloud computing* ed in caso affermativo, in che forme e con che modalità[17]. Poniamo il caso che il sistema sia acceso ed in funzione e la polizia giudiziaria d'iniziativa sia interessata a conoscere quante più informazioni possibili prima di richiedere eventualmente un decreto di perquisizione al magistrato. Un'attività invasiva di accesso interno al sistema e di utilizzo degli strumenti informatici potrebbe provocare un'alterazione del sistema stesso o dei dati ed una modifica dei *file* o del loro contenuto (soprattutto se il *file* o la "cartella" vengono aperti). In questo caso, il sistema, se stimolato da una operazione anche semplice come il click del *mouse*, autonomamente effettua una serie di operazioni in grado di modificare informazioni interne al sistema stesso. Ciò potrebbe porre in essere un'attività contrastante con il nuovo disposto dell'art. 244 c.p.p. che stabilisce la necessità di adottare *misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.* L'attività posta in essere in questo caso sembra andare oltre il semplice "sguardo esplorante" tipico dell'ispezione. Tale attività sembra andare oltre il semplice scrutamento del contenuto, delle forme, delle qualità e caratteristiche del mezzo per giungere invece ad una attività più vicina a quella tipica di perquisizione. Ad avviso di chi scrive, l'attività di ricerca di un qualcosa di preciso e circostanziato all'interno di un sistema informatico o di un *Cloud* sembra essere riferibile più all'ipotesi di perquisizione piuttosto che di "*inspectio*", mentre una ricerca più generica e superficiale che si limita alle caratteristiche esteriori sembra più vicina all'ispezione informatica disciplinata dall'art. 244 c.p.p.

3. Competenza territoriale. Una delle questioni interpretative di maggior rilievo poste dagli illeciti penali commessi mediante Internet è costituito dalla determinazione della giurisdizione e della competenza in relazione alla individuazione del *locus commissi delicti* nel *cyber*–spazio nonché ai casi in cui ricorrere o meno alla rogatoria internazionale. La rete e con essa il

16. Si veda D'AMBROSIO, ult. cit., p. 73.

17. Si veda Cass., Sez. III, 26 gennaio 2000, A., in *Mass. Uff.*, n. 217687, trattasi di una delle primissime sentenze della Suprema Corte in materia di ispezioni su dati informatici (seppur *sui generis*). In tema di mezzi di ricerca della prova, non costituisce sequestro probatorio l'acquisizione, mediante riproduzione su supporto cartaceo, dei dati informatizzati contenuti in un archivio informatico visionato nel corso di una ispezione legittimamente eseguita ai sensi dell'art. 244 c.p.p. Nel caso di specie la Corte ha ritenuto che non si versasse in un' ipotesi di sequestro in quanto non vi era stata alcuna apprensione dell'archivio informatico il quale non era stato sottratto al possessore, bensì di una semplice estrazione di copia dei dati in esso contenuti, sicché non si poneva nemmeno un problema di restituzione dei supporti cartacei realizzati.

Cloud, infatti, nella sua dimensione virtuale costituiscono un luogo parallelo rispetto a quello reale che infrange i tradizionali limiti temporali e territoriali del *tempus* e del *locus commissi delicti* e pone alcuni problemi relativi all'accesso da remoto a dati collocati in altri Paesi[18].

Il carattere sovranazionale della rete pone concreti rischi di sovrapposizione tra diverse giurisdizioni nella persecuzione penale dei reati *on line* e delicati questioni in tema di conflitti di legge nello spazio (e, correlativamente, di *bis in idem* internazionale). Non di rado, inoltre, l'autore della condotta criminosa ricorre a percorsi telematici tortuosi per accedere ai siti bersaglio al fine di depistare le indagini finalizzate alla sua identificazione.

La c.d. teoria della ubiquità consente al giudice italiano di conoscere del fatto di reato, tanto nel caso in cui sul territorio nazionale si sia verificata la condotta, quanto in quello in cui su di esso si sia verificato l'evento. Pertanto, nel caso di un *iter criminis* iniziato all'estero e conclusosi (con l'evento) nel nostro paese, sussiste la potestà punitiva dello Stato italiano. Se infatti l'applicazione della teoria dell'ubiquità porta con sé una facile risoluzione, in favore del giudice italiano, di molte delle problematiche che in fatto si possono presentare all'interprete, ben più complesso è il discorso laddove si passi dal *reato* alla individuazione e raccolta delle *evidenze* informatiche[19].

Con il diffondersi del *Cloud* e quindi del suo utilizzo anche in modo illecito, sarà sempre più frequente che polizia giudiziaria si trovi ad ispezionare un *client* che — sia pure materialmente presente sul luogo della perquisizione — non ha database o memoria in locale ma tutto il contenuto è ubicato all'estero.

Nell'ispezionare un *client* acceso con i dati tutti o parte di essi su *Cloud* e dopo aver superato le password si deve tener presente che i dati sono fisicamente conservati su server collocati in altri paesi e che la loro materiale acquisizione o il loro sequestro avviene all'insaputa dell'autorità giudiziaria del paese che ospita il sistema *Cloud*. È qui il vero punto problematico: occorre utilizzare, come prescrive la convenzione di Budapest del 2001, i canali tra autorità giudiziarie, procedere eventualmente con una rogatoria, oppure, visto che materialmente i dati sono comunque "a portata di *personal computer*" in quanto visibili e acquisibili dallo schermo del PC, si può procedere ad una ispezione o ad una acquisizione magari osservando le garanzie stabilite dal codice di procedura penale a tutela dell'integrità dei dati raccolti? Alcuni sostengono[20], che — tale *server* non viene "fisicamente toccato", dal momento che la polizia giudiziaria — operando dal *client* – si limita a richiamare *su di esso* le informazioni utili alle indagini, al fine di farne una copia;

18. In materia si veda D'Arcangelo, *La criminalità informatica ed il cybercrime nella interpretazione della giurisprudenza,* Relazione tenuta a Milano, 26 giugno 2008, *inedita*.

19. Aterno, Cajani, Costabile, Mattiucci, Mazzaraco, *Manuale*, cit., p. 417.

20. Aterno, Cajani, Costabile, Mattiucci, Mazzaraco, *Manuale*, cit., p. 413.

la polizia giudiziaria, in questo modo non forza alcuna misura di protezione, dal momento che la preesistente interconnessione tra le diverse postazioni informatiche è tale da poter affermare che il *server* è stato appositamente configurato per fornire le risposte alle richieste provenienti da tutti i *client* all'interno di una determinata rete ed, in particolare, a quello oggetto di ispezione. Occorre riflettere e verificare se, una simile attività di polizia giudiziaria, ove delegata dal pubblico ministero con motivato provvedimento di perquisizione ed ispezione dei sistemi informatici, comporti o meno profili di invalidità o pregiudichi le garanzie difensive dettate dal Codice di Procedura Penale. Allo stato, non risultano provvedimenti giurisdizionali in ambito di perquisizione di spazio *Cloud*[21] ma, potrebbe essere d'aiuto per comprendere il principio alla base del ragionamento, la giurisprudenza in tema di "instradamento" ovvero l'intercettazione delle telefonate che giungono nel paese del destinatario della chiamata senza dover intercettare l'utenza del chiamante ma captando il flusso della telefonata nel momento in cui giunge in Italia. La giurisprudenza della Cassazione in questi casi ha sempre giustificato il mancato ricorso alla rogatoria internazionale sottolineando talvolta l'opportunità di stabilire però in materia convenzioni o accordi tra Stati. È di tutta evidenza che nel caso dell'instradamento delle telefonate vi è comunque il provvedimento autorizzativo del giudice per le indagini preliminari che deve essere presente anche, *mutatis mutandis*, in caso di perquisizione e "sequestro" del *Cloud* in sede di convalida entro il termine stabilito. Diverso discorso deve farsi nel caso di repertamento di un *Cloud* che contiene il corpo del reato (es. immagini pedopornografiche). Un siffatto contenuto obbliga l'autorità giudiziaria anche alla cancellazione del materiale[22] per evitare il perpetuarsi dell'azione criminosa. In questo caso, nell'impossibilità concreta di procedere alla cancellazione certa dei *file* illeciti senza avvisare la società che gestisce il *Cloud,* una volta acceduto e verificato il contenuto è forse opportuno e più semplice, inibire l'accesso modificando le credenziali dell'account e procedendo all'acquisizione definitiva e alla cancellazione di tutti i *file* attraverso una rogatoria[23] o ad una "semplice" richiesta attraverso un contatto diretto con la società di *Cloud* (o con il *Cloud Service Provider*).

21. Sulla prassi invalsa in tema di perquisizione "live" e di accesso da remoto ad una casella di posta elettronica, Aterno, Cajani, Costabile, Mattiucci, Mazzaraco, *Manuale*, cit., p. 418.

22. Cancellazione che è sostanzialmente diversa dalla mera e materiale copia informatica da remoto.

23. In caso di necessità di provvedimento giudiziario.