GIANLUCA BRAGHÒ

LE INDAGINI INFORMATICHE FRA ESIGENZE DI ACCERTAMENTO E GARANZIE DI DIFESA

SOMMARIO: 1. Premessa. — 2. Le principali fonti normative. — 3. La Convenzione di Budapest. — 4. Gli atti d'indagine ed i mezzi di ricerca della prova del reato informatico. — 5. Le intercettazioni di comunicazioni informatiche e telematiche. — 6. Le acquisizioni documentali. — 7. La normativa in tema di conservazione dei files di log: profili critici. — 8. Spunti per una modifica legislativa al Codice della Privacy. — 9. La modifica legislativa al Codice della Privacy a seguito della legislazione Pisanu (L. 155/05). — 10. Gli accertamenti tecnici. Cenni sui principi di Digital and computer forensics.

1. Premessa.

La presente relazione non ha pretese di completezza in ordine agli argomenti trattati, ma ha l'intento di porsi quale testimonianza di esperienze sul campo, condotte nella prassi giudiziaria milanese. Ha altresì l'intento di sollevare profili critici in ordine alle carenze delle norme e degli strumenti idonei a consentire un'adeguata risposta alla proliferazione della criminalità informatica e alla prevenzione degli errori in fase investigativa, in vista di un'auspicabile riforma della normativa attualmente in vigore.

2. Le principali fonti normative.

Nell'ultimo biennio si è verificata una crescita esponenziale di procedimenti contenenti notizie di reato in tema di reati informatici.

Il primo strumento utile per un'efficace azione di contrasto è la normazione intesa quale diritto positivo formato da trattati internazionali, direttive e regolamenti UE, leggi statali e idonei a delineare le ipotesi di reato e gli strumenti di accertamento dei medesimi.

Le istanze di legalità che derivavano dall'utilizzo delle nuove frontiere tecnologiche hanno viste riconosciute le proprie pretese attraverso il

* Testo della Relazione presentata al Convegno *I delitti dell'informatica. Problemi aperti e prospettive di riforma*, tenutosi in Monza il 1º Luglio 2005.

varo di una serie di disposizioni legislative che hanno regolato una materia tuttora in continua evoluzione. Anche facendo leva sull'impulso normativo derivante da alcune direttive della UE, sono state promulgate: la legge sulla tutela penale del diritto d'autore e sugli illeciti di duplicazione e commercializzazione abusiva di prodotti industriali (novelle legislative incardinate sulla vecchia, ma pur sempre valida ed efficace, legge n. 633/41 e via via introdotte con il D.L. 518/92, con la legge 284/00 e relativi regolamenti attuativi, con successive modifiche apportate dalla c.d. legislazione urbani del biennio 2004-2005); la legge introduttiva dei reati informatici cd. « puri » n. 547/93, attraverso la quale, con la tecnica della modifica addittiva al codice penale sono state tipizzate ex novo ulteriori ed innovative fattispecie di reato; le leggi collaterali in materia di tutela della privacy (L. 675/96 e soprattutto il D. Lgs. 196/2003) e di contrasto della pedofilia anche telematica (L. 286/98); la legge introduttiva del principio della responsabilità amministrativa degli enti per reati commessi dai soggetti che agiscono per loro conto o nel loro interesse esclusivo e prevalente, ovvero che esercitino poteri di direzione, amministrazione e controllo della persona giuridica (legge 231/2001).

Come si può notare, da poco più di un decennio, il legislatore ha messo mano allo strumento legislativo seguendo due diversi criteri: la regolamentazione di settori specifici d'interesse criminale mediante l'introduzione di leggi speciali, non sempre coordinate con il codice penale; la novella del codice penale medesimo, con creazione di norme penali incriminatrici mutuate dalle fattispecie classiche in tema di violazione di domicilio e della corrispondenza, di danneggiamento e di truffa; l'adozione di testi unici innovativi che regolano organicamente la materia della privacy, la quale impinge fortemente con le norme del codice di procedura penale; la partecipazione alla stipula di trattati internazionali (la Convenzione di Budapest del 23 novembre 2001 adottata in seno al Consiglio d'Europa, per contrastare la criminalità informatica).

Dal punto di vista della teoria del bene giuridico tutelato, il legislatore ha delineato implicitamente le caratteristiche dell'illecito informatico: esso è un reato plurioffensivo che aggredisce la libertà di comunicazione e di manifestazione del pensiero (artt. 15 e 21 Cost.) e, nel contempo, il patrimonio della persona offesa.

Per quel che concerne il profilo dell'elemento materiale del reato, il delitto informatico si configura alla stregua di una condotta vietata, posta in essere sul computer e/o attraverso il computer; ove lo strumento tecnico (inteso quale insieme di software ed hardware), a seconda dei casi, può dunque atteggiarsi quale oggetto materiale del reato (cosa fisica o bene economicamente e giuridicamente apprezzabile su cui ricade la l'attività dell'autore del reato), ovvero quale cosa pertinente al reato (strumento necessario per agevolare o consumare la condotta illecita). Tale distinzione, che applica al reato informatico le nozioni classiche in materia di teoria generale dell'illecito penale, consente di effettuare una « summa divisio » fra reato informatico puro; reato informatico spurio; reato comune commesso con tecniche legate a sistemi informatici.

Nel primo concetto possono essere incluse tutte le figure d'illecito contenute nella legge 547/93, ovvero i reati d'intrusione (accesso abusivo ed ipotesi satellite), di danneggiamento, di frode informatica. In sintesi, sono quei reati in cui viene tutelato il sistema informatico quale bene patrimoniale suscettibile di attacchi esterni o di usi abusivi commessi dagli

operatori del sistema, nonché da condotte fraudolente finalizzate alla truffa. Il reato informatico puro è dunque un reato contro il patrimonio. Nella prassi commerciale l'uso massivo e la diffusione di Internet ha moltiplicato le possibilità di esposizione dei sistemi informatici ad attacchi esterni. Sul piano logico, i reati introdotti nel codice penale sono in stretta relazione fra loro. Il legislatore ha coerentemente previsto figure di illecito strumentali rispetto all'ipotesi cardine rappresentata dalla frode informatica. Nella pratica criminale difficilmente un'intrusione informatica è fine a se stessa. A meno di non confrontarsi con un hacker « puro », il quale viola il sistema per il gusto di cimentarsi con le sue misure di protezione, l'intenzione dell'agente è quasi sempre quella di « bucare » il sistema per danneggiarlo, comprometterne il funzionamento in via temporanea o definitiva, manipolare o sottrarre preziose informazioni, utilizzare i dati estrapolati abusivamente per commettere frodi, ovvero indurre l'ignaro utilizzatore del sistema a commettere per suo conto reati di duplicazione abusiva di software, servendosi del sistema informatico violato quale « ponte » per veicolare informazioni o prodotti industriali coperti dal copyright, ovvero immagini pedo-pornografiche, schermando in tal modo la propria identità e garantendosi l'impunità.

Nelle fattispecie di illecito non aggravate da particolari circostanze, la perseguibilità del reato è a querela di parte. L'opzione legislativa ha in tali casi evidenziato alcune lacune di tutela. Infatti, accade di sovente che le imprese vittime di attacchi al proprio sistema informatico preferiscono tacerne l'esistenza anziché denunziare il fatto all'Autorità giudiziaria per timore di diminuire l'immagine o la parvenza di efficienza ed affidabilità sul mercato. Ciò accade puntualmente quando destinatari di un'intrusione sono Istituti di credito, imprese di assicurazioni, grandi e medie imprese di servizi. Tali soggetti, forse per scarsa fiducia nell'azione delle forze dell'ordine e dell'A.G. nel perseguire e individuare gli autori del reato, optano per il silenzio, tentando di limitare i danni e risolvere i problemi creati dagli attacchi degli hackers con le sole proprie risorse, contribuendo così a creare un'area sommersa di reati informatici che rimarranno impuniti.

Per quel che concerne l'elemento soggettivo del reato, la legge generalmente postula il requisito del dolo generico, tipico dei reati di danneggiamento e di frode, inteso quale coscienza e volontà della condotta e dell'evento quale conseguenza di essa. Infine, i reati informatici sono tutti reati commissivi di condotta o di evento, in quanto presuppongono sempre un « *facere* » o un « *agere* » che produce un evento pericoloso o dannoso per la persona offesa.

La normazione deve prevedere anche regole precise in tema di formazione, acquisizione e valutazione delle prove c.d. informatiche.

Le peculiarità delle indagini nel settore dei reati informatici hanno condotto gli operatori del diritto a coniare i termini di informatica forense (digital forensic; computer forensic) e di prova digitale (digital evidence), concetti che indicano determinate fasi di cui si compone un'indagine informatica.

Tuttavia occorre chiarire che non è sufficiente la sola normazione a dettare compiutamente le regole del settore. In un'indagine informatica molte sono le figure professionali (ufficiali ed agenti di P.G.; ausiliari di P.G. dotati di particolari e limitate cognizioni tecniche; CTU e CTP, esperti informatici) che possono intrecciarsi con il lavoro ed i compiti del

magistrato requirente e che necessitano di specifiche regole di condotta, di linee guida e di protocolli investigativi (best practices). Alla normazione si deve affiancare la migliore prassi.

3. La Convenzione di Budapest.

È un trattato internazionale che mira a creare un sistema europeo di regole integrato ed uniforme in tema di diritto penale dell'informatica.

La Convenzione di Budapest prevede nel suo preambolo il contemperamento fra le esigenze di accertamento degli autori del reato informatico e i diritti fondamentali dell'individuo (ed in particolare il diritto alla riservatezza). Le regole che disciplinano le indagini informatiche devono essere la risultanza di una convergenza di fattori che determini l'equo contemperamento degli interessi in gioco: da un lato l'esigenza di dotare le autorità inquirenti di un efficace ventaglio di strumenti di contrasto, dall'altro l'esigenza di tutelare il trattamento dei dati personali e delle informazioni veicolate tramite reti globalizzate. Si potrebbe dire che esistono due principi non necessariamente antitetici che devono essere contemperati: proteggendo i dati personali da intrusioni investigative si protegge la vita intima di ogni individuo e, di contro, solo attraverso un'efficace azione di contrasto si tutela l'identità e la vita di relazione dell'individuo. Nel preambolo della Convenzione di Budapest si rinvengono tali dichiarazioni di principio che vengono successivamente sviluppate attraverso l'enunciazione di una serie di regole sostanziali, procedimentali e processuali cogenti per gli Stati aderenti.

La Convenzione di Budapest è programmatica e tende all'armonizzazione futura delle legislazioni nazionali dei Paesi firmatari, imponendo ai medesimi l'obbligo di adeguare le legislazioni interne sul piano del diritto criminale sostanziale, mediante l'adozione di fattispecie incriminatici che ricalcano le figure tipiche dei reati informatici puri (reati contro l'integrità, la disponibilità, il trattamento lecito di dati informatici e dei sistemi informatici; reati di frode e di falsificazione informatica) e « spuri » (furti d'identità e truffe con carte di credito; reati in materia di diritto d'autore e di proprietà intellettuale in genere; reati di pedopornografia on line).

La Convenzione prevede inoltre per gli Stati firmatari l'obbligo di adottare misure repressive adeguate ed effettive, che assicurino la reale afflittività delle sanzioni, nonché di dotarsi di una legislazione che affini gli strumenti giudiziari di contrasto alla criminalità informatica (intercettazioni, perquisizioni e sequestri; acquisizione di dati dai service provider; obbligo di conservazione, di segretezza, di custodia, di congelamento dei dati richiesti dall'autorità inquirente).

È forse questa la quaestio dolens rispetto all'attuale disciplina italiana in tema di privacy (art. 132 del D.Lgs. 196/2003), assolutamente non conforme ai dettami della Convenzione e dunque carente in tema di disciplina di conservazione e trattamento dei files di log per finalità di accertamento e repressione dei reati informatici. Sul punto la legge nazionale viola il principio determinato dalle norme di diritto internazionale generalmente riconosciute, sancito dall'art. 10 della Cost. (nel caso di specie: pacta sunt servanda) e dunque è affetta da illegittimità costituzionale nella parte in cui non prevede una disciplina specifica per la con-

servazione e il trattamento dei dati relativi alle connessioni telematiche ed informatiche.

La Convenzione, infine, affronta in maniera organica altri due profili critici che si incontrano sul piano operativo in ambito di indagini informatiche: la competenza giurisidizionale dovuta alla dematerializzazione e alla delocalizzazione dell'illecito; la cooperazione internazionale fra diverse forze di polizia e fra le autorità giudiziarie nazionali, con particolare riferimento ai temi della mutua assistenza finalizzata a favorire l'accesso transfrontaliero ai dati informatici immagazzinati nel territorio di uno degli Stati aderenti al trattato, della raccolta in tempo reale e dell'intercettazione di dati relativi al contenuto delle comunicazioni informatiche e telematiche, nonché della creazione e della messa a disposizione di ogni Stato aderente alla convenzione di un punto di contatto, disponibile 24 ore al giorno e 7 giorni su sette, per assicurare un'assistenza immediata per le indagini relative a reati connessi a sistemi e dati informatici o per la raccolta di prove in formato elettronico di un reato (anche comune, ma commesso con tecnologie informatiche).

4. Gli atti d'indagine ed i mezzi di ricerca della prova del reato informatico.

Nella congerie degli strumenti a disposizione dell'A.G. per rendere efficace l'azione di contrasto dei crimini informatici si annoverano: le indagini tecniche, le acquisizioni documentali, gli accertamenti tecnici, le perquisizioni ed i sequestri, gli accertamenti bancari, gli strumenti classici di controllo del territorio (osservazione, pedinamento e controllo delle persone), gli interrogatori ed i confronti, le individuazioni di persone o cose, le sommarie informazioni dalle persone informate sui fatti.

Le indagini informatiche rendono peculiari le prime tre categorie degli strumenti testé menzionati, mentre non contemplano diversità per quel che concerne gli atti d'indagine classici, sempre utilizzabili in qualunque caso, qualora l'organo inquirente ne ravvisi l'utilità. Con un'unica precisazione. La sequenza degli atti non è stata posta a caso, ma è ordinata secondo un criterio logico e cronologico indicante il percorso paradigmatico dell'indagine informatica tipica e completa, che ha il suo incipit da indagini tecniche (intercettazioni telematiche) e si conclude, una volta identificata la persona da sottoporre alle indagini, con l'interrogatorio della medesima, prodromico alle sue allegazioni difensive e, in definitiva, a consentire al P.M. di orientarsi correttamente circa le determinazioni inerenti l'esercizio dell'azione penale.

Occorre, pertanto, soffermarsi sui seguenti atti d'indagine: le intercettazioni di flussi di comunicazioni informatiche e telematiche; le acquisizione documentali e gli accertamenti tecnici.

5. Le intercettazioni di comunicazioni informatiche e telematiche.

Costituiscono lo strumento indispensabile delle indagini tecniche. Sono disciplinate dagli artt. 266, 266-*bis*, 267, 268, 269, 270, 271 c.p.p.

Sono autorizzate dal GIP su motivata richiesta del P.M.

La necessità di tali strumenti di ricerca della prova scaturisce, di solito, dal monitoraggio preventivo effettuato sulla rete Internet dagli organi di Polizia giudiziaria specializzata.

Le esigenze investigative che vengono soddisfatte dalle indagini tecniche sono varie. Può accadere di dover monitorare tutto il traffico informatico generato da un singolo utente, intercettando tutte le informazioni veicolate da qualsiasi tipo di connessione (analogica, ISDN, ADSL, WAP, servizio di posta elettronica etc. etc.), come si può rendere opportuno effettuare una selezione di un particolare flusso di dati provenienti da una specifica area o da un determinato server provider, ovvero da un intero dominio, allo scopo di acquisire informazioni utili da porre in relazione a singole utenze che si connettono alla sorgente intercettata, nonché al fine di accertare le finalità delittuose per cui la sorgente stessa è stata creata ed utilizzata.

Più di rado, le investigazioni richiedono l'intercettazione di traffico generato da postazioni specifiche, quali ad esempio gli Internet points situati in luoghi aperti al pubblico (bar, centri ed esercizi commerciali, stazioni ed aeroporti, aree di servizio), utilizzati dagli autori dell'illecito informatico per rendere estremamente difficoltosa la loro identificazione.

Al fine di garantire la riservatezza dei dati acquisiti a seguito delle intercettazioni informatiche, è opportuno criptare i dati con algoritmi o con password accessibile esclusivamente agli operatori del sistema o a delegati dell'organo inquirente.

Come si può notare, le indagini tecniche sono uno strumento molto duttile d'investigazione. Gli esempi sopra riportati non sono che una minima parte di quello che la prassi investigativa richiede.

La legge introduttiva dei reati informatici puri (art. 11 legge 23 dicembre 1993 n. 547) ha opportunamente novellato il sistema codicistico delle intercettazioni, aggiungendo quelle relative alla comunicazione informatica e telematica.

La disciplina si conforma alle regole delle intercettazioni classiche, con alcune particolarità.

In primo luogo, le intercettazioni informatiche sono riferibili sia agli illeciti informatici puri, che ai delitti comuni, ma commessi mediante l'impiego di tecnologie informatiche e telematiche. La peculiarità della disciplina risiede nell'esclusione, per tale tipologia d'intercettazione, del limite di ammissibilità dell'atto d'indagine in considerazione della pena edittale del reato prevista dal comma I lett. *a*) dell'art. 266 c.p.p., qualora l'impiego del mezzo informatico e della tecnologia telematica sia lo strumento attraverso il quale viene realizzata la condotta penalmente rilevante. Tale previsione è in linea con la ratio dell'intera disciplina dettata per i reati informatici, i quali difficilmente superano i limiti edittali previsti dal citato comma.

Inoltre, la normativa prevede che per l'esecuzione delle operazioni d'intercettazione il P.M. può disporre che le stesse siano compiute mediante impianti appartenenti a privati (art. 268 comma 3-*bis* c.p.p.), Tale locuzione deve essere posta in relazione con il comma 3 dell'art. 268 c.p.p., il quale, diversamente prevede che, salvo eccezionali casi motivati da esigenze d'urgenza dell'esecuzione, ovvero da insufficienza o inidoneità delle strutture tecniche disponibili, le operazioni d'intercettazione devono essere compiute esclusivamente per mezzo degli impianti

installati nella Procura della Repubblica, a pena d'inutilizzabilità dei risultati delle stesse, in violazione di tali previsioni normative (art. 271, I comma, c.p.p.).

Se è vero che il comma 3-*bis* dell'art. 268 c.p.p., non menziona l'accenno all'ubicazione degli impianti alternativa a quella della Procura della Repubblica, è altrettanto corretto ritenere che la locuzione sia riproduttiva del significato indicato dalle parole « mediante impianti di pubblico servizio o in dotazione alla polizia giudiziaria », ove, per il caso delle intercettazioni classiche, essa sta a indicare un diverso luogo di ubicazione delle operazioni di ascolto, sotto il controllo indiretto del P.M., e dunque al di fuori dei locali della Procura della Repubblica.

Inoltre, la sanzione dell'inutilizzabilità è prevista esclusivamente per la violazione del disposto di cui al comma 3 dell'art. 268 c.p.p., ad ulteriore conferma che il P.M. può eseguire le operazioni d'ascolto telematico presso gli impianti di privati ubicati in un qualsiasi luogo ritenuto opportuno.

Su quest'ultimo punto, la divergenza di disciplina con le intercettazioni telefoniche è massima. Infatti, in questo ultimo caso, quand'anche il P.M. si avvalga di impianti non installati presso la Procura della Repubblica procedente, dovrà comunque utilizzare impianti di pubblico servizio o in dotazione alla Polizia giudiziaria, intendendosi sempre quali attrezzature in uso a strutture pubbliche di intelligence (servizi segreti, Ministero dell'Interno) o alle forze dell'ordine. In nessun caso sarà consentito ubicare la sala ascolto presso sedi gestite da privati. Il P.M. potrà comunque autorizzare con apposito decreto la Polizia giudiziaria a reperire i dispositivi d'intercettazione di cui è priva, locandoli da operatori privati.

Quella appena descritta non è una differenza di disciplina di poco rilievo, se si ha riguardo a tutta la casistica giurisprudenziale della Suprema Corte di Cassazione in tema di inutilizzabilità dei risultati delle intercettazioni classiche, le cui operazioni sono eseguite al di fuori degli impianti installati nella Procura, in mancanza o in difetto di decreto motivato (e reiterato nelle richieste di proroga) del P.M. circa l'urgenza o l'indisponibilità delle postazioni d'ascolto in dotazione all'A.G. I recenti irrigidimenti formalistici della Suprema Corte sul punto, motivati dal principio del controllo diretto del P.M. sulle operazioni d'ascolto a tutela della libertà di manifestazione del pensiero e di ogni forma di comunicazione *ex* artt. 15 e 21 Cost., non tengono conto che tale ratio interpretativa è radicalmente inapplicabile alle intercettazioni informatiche e dunque non può ergersi a principio cardine in detta materia, a meno di non considerare la disciplina relativa alle intercettazioni telematiche ed informatiche speciale, rispetto a quella riferibile alle ordinarie intercettazioni telefoniche.

Opzione interpretativa difficilmente percorribile, avuto riguardo alla norma di coordinamento indicata dall'art. 266-*bis* c.p.p.

Si deve evidenziare, infine, che le intercettazioni di flussi di comunicazioni relative a sistemi informatici o telematici, presentano costi economici decisamente più contenuti rispetto alle intercettazioni telefoniche ed ambientali.

6. Le acquisizioni documentali.

Sono atti d'indagine complementari ai sequestri (artt. 253 e seguenti c.p.p.), che hanno un grande rilievo ed utilità nell'indagine informatica. Sono equiparabili ai decreti di acquisizione dei tabulati telefonici destinati ai gestori di telefonia.

Usualmente l'hacker o il cracker lasciano alcune tracce delle loro scorribande telematiche. L'acquisizione dei files di log relativi alle connessioni presso gli archivi dei gestori dei servizi resi su Internet costituisce uno strumento efficace e rapido per giungere tramite l'indirizzo I.P. alla fonte della connessione.

Si differenziano dalle classiche richieste di esibizione documentale emesse con decreto motivato del P.M., per l'oggetto dell'acquisizione.

Sul piano normativo, esse si distinguono dalle intercettazioni, perché hanno lo scopo di acquisire alle indagini i risultati e gli elementi esterni, identificativi delle comunicazioni fra sistemi informatici. Il gestore del servizio sarà obbligato ad ottemperare a seguito della mera presentazione del decreto del P.M., senza che l'organo inquirente per l'esecuzione dell'atto istruttorio debba richiedere l'autorizzazione al GIP, come nel caso delle intercettazioni o dei dati relativi ai tabulati telefonici, in virtù del diverso e più limitato livello d'intrusione nella sfera di riservatezza del cittadino che ne deriva e che non postula l'osservanza della più rigida e formalizzata procedura prevista in tema d'intercettazione delle comunicazioni.

I risultati di tali atti possono essere utilizzati in dibattimento, alla stregua di comuni documenti (art. 234 c.p.p.).

7. La normativa in tema di conservazione dei files di log: profili critici.

La recente introduzione del T.U. sulla privacy ha di fatto deregolamentato la delicata materia. Il testo attualmente in vigore, a seguito di una modifica legislativa (l. 354/2004) ha in pratica scisso testualmente la disciplina in tema di acquisizione e conservazione dei dati relativi al traffico telefonico (c.d. tabulati telefonici) da quella relativa ai dati sulle connessioni informatiche e telematiche (C.D. FILES DI LOG) originando di fatto un preoccupante vuoto normativo la cui nefasta azione si riverbera sulla possibilità stessa di effettuare le indagini informatiche in un numero elevatissimo di casi. Infatti, l'indagine informatica tipica è un'investigazione a ritroso (tracing) che conduce l'operatore di P.G. e il PM a risalire alla fonte della connessione. Si stabilisce quindi un rapporto simbiotico fra risultato investigativo ed acquisizione del dato relativo alla connessione. Risulta oltremodo necessario disciplinare in modo organico i rapporti fra i fornitori dei servizi di connessione (providers) e la magistratura, stabilendo, obblighi e diritti delle parti in causa, nonché procedure di raccolta, conservazione, trattamento, divulgazione, cancellazione dei dati. Il codice della Privacy è in tale settore del tutto carente, come lo è per quanto attiene agli obblighi di garanzia del gestore telefonico o telematico in relazione a possibili attività criminali attive sulle proprie reti. L'assenza di regole chiare che rendono equilibrato l'assetto degli interessi in gioco è il principale fattore criminogeno nel settore dei reati in-

formatici. La carente normativa sulla privacy, nel dichiarato intento di tutelare la riservatezza, raggiunge il risultato opposto: favorire la criminalità che utilizza i dati personali altrui per proprio illecito profitto, facendosi beffa di quella stessa tutela del dato sensibile che il legislatore ha inteso proteggere soltanto rispetto alle intrusioni investigative.

Si è assistito ad un vero e proprio svuotamento dei poteri d'indagine del PM in tema di acquisizione dei tabulati telefonici, attraverso una disciplina a tratti bizzarra, laddove prevede un'incomprensibile scissione temporale per la conservazione dei dati nei commi 2 e 3, del tutto irrilevante per chi detiene i reports (ed infatti come può il provider preventivamente conservare in maniera temporalmente differenziata i dati del traffico telefonico se non conosce a priori la tipologia di delitto per cui viene attivata la richiesta?), a tratti priva di norme chiare in settori vitali d'interesse investigativo (fra i tanti rilievi critici: è assente la normativa in tema di acquisizione dei files di log. Non si è previsto il potere del PM di richiedere con decreto motivato l'acquisizione dei tabulati al gestore telefonico nei casi di urgenza, come accade per le intercettazioni. Non sono previste norme a garanzia dell'indagato circa l'autenticità e la genuinità del dato informatico fornito dal provider).

Attualmente, l'acquisizione dei dati relativi al traffico telematico ed informatico, nonché le tracce delle connessioni in rete recanti l'identificazione della postazione chiamante o interconnessa, possono essere acquisite dal PM con decreto motivato ai sensi dell'art. 256 c.p.p. da comunicarsi direttamente al gestore competente. Dopo una prima oscillazione applicativa che si conformava alla disciplina prevista per i tabulati telefonici, anche a seguito della novella legislativa del tutto affrettata (D.L. 45/04 convertito in L. 354/04), l'ufficio GIP ha sempre espresso il non luogo a provvedere sulle pedisseque richieste del PM in tema di files di log.

Ma la conservazione in capo al PM di tale autonomo potere investigativo assomiglia da vicino alla vittoria di Pirro sui Romani. Il risvolto giuridico è l'estremo depotenziamento dell'attività d'indagine.

Infatti, i gestori non sono obbligati a conservare i files di log per precipue finalità di accertamento e repressione dei reati (art. 132 T.U.). Si può anche con certezza affermare che alcuni providers non « loggano » tout court le connessioni, ovvero non conservano le tracce informatiche delle connessioni telematiche per policy aziendale.

L'unica norma che può essere utilizzata in materia è il disposto dell'art. 123 T.U., il quale permette la conservazione dei dati relativi al traffico riguardanti abbonati ed utenti a fini di fatturazione per l'abbonato o di documentazione in caso di contestazione della fattura o per la pretesa di pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale.

Ne consegue che paradossalmente in materia di contenzioso extrapenale si prevede la possibilità di un congelamento indeterminato dei dati eventualmente pluriennale, avuto riguardo ai tempi della definizione delle controversie civili ed amministrative.

Una previsione di conservazione « elastica » è stata dettata per i dati di traffico inerenti i servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto (prefissi telefonici con numerazione iniziale 709-702-166-899 etc. etc.), nella misura e per la durata necessaria

ai fini di commercializzazione di tali servizi e solo previo consenso dell'utente o dell'abbonato, sempre revocabile in ogni momento.

Tale norma costituisce l'unico riferimento circa la conservazione dei dati di traffico telematico, fra cui sono ricompresi i files di log. Il rischio è di ottenere una risposta negativa che fa seguito alla richiesta di acquisizione. Tale risposta negativa paralizza le investigazioni tecniche che in molti casi non possono essere proseguite. Dubbia è la possibilità di costringere giuridicamente il provider a fornire i dati, ancorché in suo possesso, atteso che egli non è obbligato a conservarli. Del pari dubbia è, infine, la legittimità della policy aziendale di alcuni providers di conservare i files di log per tempi superiori o con modalità non previste dall'art. 123 T.U., pur al commendevole fine di agevolare il lavoro dell'A.G. in caso di indagini preliminari in corso, poiché il titolare o il responsabile del trattamento dei dati informatici potrebbero incorrere nelle sanzioni penali previste dal T.U. sulla Privacy.

8. Spunti per una modifica legislativa al Codice della Privacy.

Si coglie l'occasione per tentare qualche spunto di modifica legislativa che riconduca a razionalità il sistema. Il legislatore potrebbe specificare:

Dopo il comma 5 dell'art. 132 D. Lgs. 196/2003 sono aggiunti i seguenti commi:

Comma 6. I dati relativi alle connessioni telematiche e alle tracce informatiche di tali connessioni sono conservati dal fornitore per finalità di accertamento e repressione dei reati nei termini e con i limiti previsti nei commi 2 e 3.

Comma 7. Entro i termini previsti nei commi 2 e 3 i dati sono acquisiti presso il fornitore con decreto motivato del PM di sua iniziativa o su istanza della persona sottoposta alle indagini, della persona offesa, o dei loro difensori, secondo le forme previste dall'art. 256 c.p.p. Il fornitore certifica l'autenticità dei dati comunicati all'A.G. e la loro esatta corrispondenza rispetto a quelli conservati negli archivi.

Comma 8. il fornitore è tenuto all'obbligo del segreto in relazione ai dati richiesti dall'A.G. Il fornitore è tenuto altresì a garantire l'integrità dei dati richiesti per un tempo non superiore a novanta giorni, salvo la possibilità di proroga del termine su richiesta motivata dell'A.G. e comunque non oltre il termine di scadenza previsto per la durata delle indagini preliminari.

Comma 9. Sulle richieste provenienti dalle parti private, il PM provvede entro 5 giorni dal deposito dell'atto presso la segreteria. In caso di rigetto, è ammessa opposizione al GIP nelle forme e nei modi stabiliti dagli artt. 127 e 263, V comma, c.p.p. Il GIP, se ritiene infondato il rigetto, accoglie l'opposizione e dispone che il PM provveda conformemente all'istanza entro un termine non superiore a 10 giorni.

Rationes dell'innovazione legislativa.

• Colmare un grave vuoto legislativo che vulnera la fruttuosità delle investigazioni in un numero sempre crescente di reati informatici e di reati commessi con tecnologie telematiche. Infatti a seguito delle modifi-

che al codice della privacy apportate con l. 354/04 di conversione del D.L. 45/04, non è affatto disciplinata la materia inerente l'acquisizione dei files di log e degli indirizzi I.P. ed in particolare non vi è alcun obbligo del gestore di conservare tali dati che sono fondamentali per la prosecuzione delle indagini.

• Permettere all'Italia di conformarsi alle prescrizioni della Convenzione di Budapest, di prossima entrata in vigore (come ad esempio il c.d congelamento dei dati).

• La modalità di acquisizione dei dati è affidata al PM (come lo è nell'attuale disciplina), atteso che tali dati non sono per nulla assimilabili ai tabulati telefonici e sono dei veri e propri documenti informatici che preesistono alle indagini e vengono richiesti al gestore, il quale si impegna a comunicarne l'autenticità (per evitare contestazioni in ordine alla genuinità della prova).

• Sono previsti poteri d'intervento delle parti private e del GIP in caso di rigetto infondato e immotivato del PM o di sua inazione, con una disciplina che ricalca pedissequamente quella del sequestro penale. Il preventivo vaglio del PM è necessario per eliminare le richieste infondate, palesemente erronee o dilatorie, ovvero quelle pregiudizievoli per le indagini. Il controllo del GIP è dunque di legalità sull'operato del PM in ossequio ai principi informatori del nostro diritto processuale penale (parità d'armi fra accusa e difesa; tutela della p.o. dal reato; celerità ed economia processuale, giusto processo).

9. La modifica legislativa al Codice della Privacy a seguito della legislazione Pisanu (L. 155/05)

Non a caso si è voluta lasciare intatta la parte della relazione che descriveva i profili critici della disciplina in tema di data retention prima dell'introduzione del pacchetto c.d. Pisanu. L'accertamento dei crimini informatici non può prescindere da un aspetto essenziale dell'indagine telematica: l'acquisizione del dato conservato negli archivi dei gestori e dei fornitori di connettività.

Inoltre dal confronto del testo della legge, si può constatare che alcuni spunti relativi alle modifiche proposte in tema di codice della privacy sono state recepite dal legislatore, seppure in sede di misure di urgenza per contrastare le attività terroristiche.

Per quel che qui è di utilità, occorre evidenziare che il D.L. 144/05 ha profondamente inciso sulla disciplina vigente in tema di conservazione dei dati, novellando l'art. 132 del D. lgs. 196/03. È del pari da evidenziare che anche la novella legislativa non è immune da critiche e da illogicità, probabilmente dettate dalla fretta con la quale si è soliti emanare leggi che incidono su beni essenziali del cittadino e sui poteri d'indagine della magistratura.

È indubbio che la nuova formulazione dell'art. 132 del T.U. privacy, ricomprendendo i dati relativi al traffico telematico nel novero dei dati da trattare e da conservare, pone termine a quel vuoto legislativo che inficiava la fruttuosità delle indagini informatiche. Allo stato attuale, la P.G., la magistratura inquirente e le parti processuali tutte possiedono lo strumento legislativo attraverso cui pervenire all'acquisizione dei files

di log (data log ed access log), la cui apprensione ed analisi è di fondamentale importanza per la prosecuzione delle indagini informatiche.

Si analizzano le innovazioni più salienti.

Il termine previsto per la conservazione dei dati è di mesi sei, prorogabile di altri sei mesi per i delitti informatici « puri », ovvero quelli compiuti in danno di sistemi informatici e telematici. Sono esclusi dalla prorogatio semestrale i dati telematici relativi a reati commessi mediante l'utilizzo di sistemi informatici o telematici. Tale esclusione per i c.d. reati informatici « spuri » e per i reati comuni commessi con l'uso di tecnologie informatiche risulta di difficile comprensione, se non in un'ottica di difetto di coordinamento con il disposto dell'art. 266-*bis* c.p.p. (in tema di intercettazioni telematiche) dovuta alla fretta della compilazione del testo di legge.

Si reintroduce in capo al PM, entro il termine originariamente previsto, il potere di richiedere al gestore e al fornitore di servizi di connettività i dati relativi sia al traffico telefonico (c.d. tabulati telefonici) sia al traffico telematico (dati di log). Dopo la scadenza del termine originariamente posto per legge, solo il GIP può autorizzare l'acquisizione dei dati richiesti con decreto motivato e solo se sussistano sufficienti indizi dei delitti di cui all'art. 407, comma 2, lett. *a*) del c.p.p., nonché dei delitti informatici « puri ».

Si prevede la possibilità di azione d'urgenza diretta dal PM anche quando la competenza a rilasciare l'autorizzazione spetta al GIP in via ordinaria. In tali evenienze il PM dovrà, a pena di inutilizzabilità dei dati in sede processuale, richiedere la convalida al GIP immediatamente e comunque non oltre le ventiquattro ore, attraverso un procedimento che ricalca la disciplina in materia di intercettazioni telefoniche in via d'urgenza.

In conclusione si può affermare che la legge 155/05 ha introdotto delle modifiche essenziali per la razionalità della disciplina della data retention anche se una disciplina organica in materia verrà presto introdotta attraverso una direttiva comunitaria di prossima emanazione (entro il 31.12.2005), la quale porrà nuove regole su tale delicata materia.

10. Gli accertamenti tecnici. Cenni sui principi di Digital and computer forensics.

Particolare importanza riveste il ricorso ad enti specializzati, dotati di strutture e uomini in grado di eseguire consulenze utilizzabili nella futura fase processuale su sistemi software ed hardware posti sotto vincolo di sequestro probatorio o preventivo durante le indagini preliminari.

Il complesso di attività di accertamento tecnico in materia informatica prende il nome anglosassone di « forensic o forensics » e prevede rigorose regole di acquisizione e conservazione della prova, prima di procedere all'accertamento in senso proprio. Tali atti d'indagine sono utilizzati per accertare le modalità della condotta criminosa, la presenza di eventuali correi, l'entità del danno provocato dal reato, ovvero per escludere alcune ipotesi di reato inizialmente formulate dall'organo inquirente.

Hanno, di norma, natura ripetibile e dunque non soggiacciono alle regole stabilite dall'art. 360 c.p.p., circa l'avviso e la partecipazione di consulenti tecnici di parte sotto sanzione di inutilizzabilità dei risultati in

dibattimento. La natura ripetibile dell'accertamento è un dato controverso in dottrina.

I principi dell'informatica forense possono essere sintetizzati in:

- Materialità (immaterialità) del dato digitale;
- Chain of custody in tema di acquisizione della prova informatica, ovvero documentazione di tutte le operazioni che vengono eseguite in modo tale da giustificare il dettaglio di ogni operazione compiuta (c.d. catena di custodia);
- Congelamento probatorio dei reperti (si lavora sulle copie);
- Ripetibilità degli esami sui reperti;
- Operazioni di accertamento tecnico da sviluppare in appositi laboratori attrezzati.

Gli esperti dovranno operare secondo protocolli internazionali (c.d. linee guida) assicurando qualità e integrità delle prove.

Le linee guida e le prassi applicative, nonché le modalità di svolgimento degli accertamenti tecnici e peritali devono conformarsi alle norme di procedura penale in tema di valutazione delle prove (artt. 187-192 c.p.p.).

Vige il principio del libero convincimento del giudice, purché adeguatamente motivato. Il giudice è e resta peritus peritorum. Le prove scientifiche non rivestono valore legale precostituito, ma sono credibili nella misura in cui è verificabile la coerenza logica delle argomentazioni che conducono alle conclusioni e nella misura in cui esse sono riconducibili a metodi di accertamento che appartengono al patrimonio specialistico accettato dalla comunità scientifica in un dato momento storico.