Diritto, crimini e tecnologie

MARIA CONCETTA DE VIVO, GIOVANNA RICCI*

SOMMARIO: *1. Introduzione: l'investigatore e le indagini – 2. Criminologia e* computer crime *– 3. Pedopornografia* on-line*: la normativa – 3.1. Pedopornografia* on-line*: i dati – 3.2. Pedopornografia* on-line*: aspetti di* criminal profiling *– 4. I reati commessi con l'uso del pc: il* cyber *terrorismo – 4.1. Terrorismo e* cyber *terrorismo – 4.2. Normativa antiterrorismo – 4.3. Possibili conseguenze del* cyber *terrorismo – 5. Profili vittimologici del reato informatico – 6.* Computer forensic *e tracciabilità – 7. (continua)* Privacy*, anonimato, anonimato e identificazione: il problema dell'IP, anonimato e quadro normativo, diritto all'oblio – 8. Prova – 9. (continua) Prova e* computer forensic*. Prova nel/del reato informatico – 10. Analisi forense.* Best practices*. Ispezione e sequestro – 11. Responsabilità per violazione delle* best practices *– 12. Prova e riferimenti normativi – 13. Prova e documento informatico – 14. Responsabilità – 15.* File *di* log *– 16. Casi di studio – 17. Informatica e prevenzione dei reati – 18. Etica professionale e* computer forensic

1. INTRODUZIONE: L'INVESTIGATORE E LE INDAGINI

"Non c'è alcun ramo delle scienze investigative così poco praticato,
eppure tanto importante, qual è l'arte d'interpretare le orme"
Sherlock Holmes

Da tempo ormai la tecnologia informatica ci offre la possibilità di compiere azioni in maniera semplice in tempi brevissimi, avendo noi del tutto acquisito le nuove tecnologie di comunicazione e divulgazione di notizie; questo grazie alla telematica, che vede l'incontro tra l'informatica e la telecomunicazione dando origine alla semplificazione del quotidiano in molti settori.

Internet e le ICT hanno già modificato moltissimi settori: dall'*e-commerce*, alla *e-bank*; dalla Borsa *on-line* alla telemedicina, dall'intrattenimento e divertimento per giungere anche all'apprendimento universitario attraverso i corsi di *e-learning*.

* M.C. De Vivo è ricercatrice di Diritto privato presso l'Università degli Studi di Camerino; è docente di Diritto dell'informatica e di Diritto dell'economia e dell'amministrazione digitale presso la Facoltà di Giurisprudenza e di Diritto delle nuove tecnologie presso la Facoltà di Scienze e tecnologie della stessa Università. G. Ricci è ricercatrice in Medicina legale presso l'Università degli Studi di Camerino; è docente di Criminologia e bioetica presso la Facoltà di Giurisprudenza.

I nativi digitali assimilano le conoscenze in maniera del tutto naturale senza nemmeno esigere spiegazioni nel merito.

Questi strumenti hanno agevolato la vita delle persone e accelerato lo sviluppo delle comunicazioni, ma hanno anche coinvolto soggetti, generalmente già devianti, ad un uso distorto del mezzo informatico o *misuse*, fino ad arrivare alla commissione di reati via *web*.

Analizzando le più frequenti violazioni della legge penale emerge che il mezzo informatico viene incongruamente usato per compiere atti illeciti quali truffe, diffusione di materiale pedopornografico o per compiere delitti contro la personalità dello Stato e molti altri reati.

Da ciò emerge che l'intelligenza dell'investigatore e la sua conoscenza del mezzo informatico appaiono elementi imprescindibili per contrastare efficacemente la criminalità moderna e portare alla soluzione dei casi giudiziari.

Sarebbe anacronistico che la giustizia non potesse beneficiare di ausili così potenti per agevolare la cattura di un delinquente o per appurare un'ipotesi investigativa/difensiva difficile da provare con i mezzi consueti di indagine quali la testimonianza, i rilievi sulla scena del crimine, i reperti biologici di laboratorio ecc.

Hercule Poirot e le sue "celluline grigie" della famosa giallista Agatha Christie rappresentano uno stereotipo di investigatore in parte superato.

Questo contesto costringe gli investigatori a confrontarsi quotidianamente con le nuove tecnologie sia informatiche sia comunicative, tant'è che attualmente, passando dall'era analogica a quella digitale, dobbiamo verificare che, anche nel settore delle indagini giudiziarie, le nuove tecnologie assumono un ruolo predominante, se adeguatamente assunte dall'inquirente durante le fasi di indagini. Ed è proprio sul campo che nasce l'esigenza di un sapere scientifico e tecnologico che impone una riforma delle figure professionali in gioco. L'investigatore alla vecchia maniera avrà ancora un ruolo fondamentale, ma soltanto rapportando il suo sapere e la sua sensibilità umana con il dato tecnico scientifico per trarre le conclusioni migliori, tagliando fuori tutti coloro che si improvvisano inquirenti o che non hanno una professionalità idonea strutturata.

Le parti in causa necessitano ciascuna di approfondimenti investigativi peculiari al proprio caso; se l'investigatore non compie tutti i passaggi necessari quali il rilevamento, il repertamento e la conservazione della prova da usare in giudizio, questi decadranno, ciò anche alla luce dei tre gradi di giudizio vigenti. In Italia questa eventualità sta avvenendo molto spesso soprattutto nel giudizio di Assise di Appello, dove la prova utilizzata in primo

grado risulta successivamente inutilizzabile a causa del cattivo repertamento e della inoculata conservazione da parte degli inquirenti.

Emerge così che la tecnologia informatica entra prepotentemente nelle indagini criminali in due modi: come elemento costitutivo del reato (pedopornografia *on-line*, *cyber* terrorismo ecc.) e come strumento di comunicazione del reo (*facebook*, *Twitter*, ecc.).

Ne consegue che:

- l'investigatore dovrà essere in grado di conoscere il mezzo informatico per verificare la violazione di legge *on-line*, conoscere il capo di imputazione in base alla scarna normativa che regola le violazioni via *web*, e formulare una accusa/difesa del soggetto indagato;
- l'investigatore, e ciò è valido per qualsiasi tipo di reato, dovrà considerare l'ipotesi in cui il reo abbia usato il computer per comunicazioni personali (*facebook*, *e-mail*, ecc.) facendo rivelazioni fondamentali per le indagini.

Affiora immediatamente l'importanza dell'analisi del mezzo informatico.

I media, a volte, contribuiscono a condizionare pesantemente il reale presentando gravi delitti sotto forma di intrattenimento, senza pensare che la realtà è molto più complessa nella sua imprevedibile casualità.

Lo scopo principale della criminologia è proprio quello di individuare il delinquente, studiarne il comportamento deviante ed assicurarlo alla giustizia, e poiché questo studio rientra in un ambito multidisciplinare, si analizzeranno elementi medici, giuridici, sociologici, economici, psichiatrici coinvolti nello svolgimento dell'azione delittuosa. Sarebbe assurdo non integrare questa disciplina con le novità tecniche che l'uso del pc può fornire nella risoluzione dei casi giudiziari.

In realtà la *computer forensic* è uno strumento prezioso a disposizione dell'investigatore che, arricchendo il suo bagaglio culturale e professionale, gli permette di affrontare l'evento criminoso nel modo più adeguato possibile, col fine unico di giungere alla soluzione del caso ed alla punibilità del delinquente.

Quello però che le tecnologie non possono fare è sostituire la preziosa sensibilità, tutta umana, dell'investigatore.

Ne è una dimostrazione il fatto che i casi verificatisi in questi ultimi anni (si pensi al caso Scazzi, al caso Yara, al caso Melania Rea, per citare i più

"articoli/devivo" — 2012/4/5 — 10:45 — page 28 — #28

tristemente noti)[1] hanno evidenziato come, pur con l'aiuto delle moderne tecnologie, i tempi di indagine (e non di risoluzione del caso!) invece che accorciarsi sembrano dilungarsi all'inverosimile.

Si ribadisce che la sola tecnologia non può essere in grado di dare risposte automaticamente immediate, ma questa combinata con il fattore umano, può risultare determinante per la soluzione dell'evento criminoso e quindi vincente.

2. Criminologia e computer crime

"I computer sono incredibilmente veloci, accurati e stupidi.
Gli uomini sono incredibilmente lenti, inaccurati e intelligenti.
L'insieme dei due costituisce una forza incalcolabile"
Albert Einstein

La rivoluzione digitale caratterizza il XXI secolo e rappresenta il mutamento del concetto di comunicazione, con nuovi scambi di informazioni in tempo reale e trasmissioni di notizie repentine; ciò ha modificato, non solo il modo di comunicare, ma anche il sistema sociale dei rapporti tra soggetti in tutti gli ambiti.

In un'ottica prettamente sociologica, a partire dalla fine degli anni '80, sulla base di un livello geopolitico, siamo passati da uno scenario bipolare ad uno multicentrico, e ciò ha rappresentato un fenomeno dinamico chiamato Globalizzazione.

In questo contesto le ICT, Informazioni, Comunicazioni e Tecnologia, divengono il fulcro del sistema mondiale caratterizzato da una complessità delle infrastrutture umane e dei piani economici, qualificando la globalizzazione come un processo bidirezionale non reversibile[2].

Questo apparato comunicativo, abbattendo ogni frontiera geografica e fisica, ha sì agevolato grandemente i contatti in ogni ambito, ma ha dato a

[1] Molti altri ce ne sono stati ma hanno avuto un impatto mediatico minore. Ad esempio il caso Bertolaso, in cui la Procura si indirizzò anche sul fronte delle tecniche investigative di *computer forensic* a causa di perquisizioni che portarono all'acquisizione di copia della memoria contenuta nell'*hard disk* del computer della giornalista di Libero, Roberta Catania. Per approfondimenti sulla documentazione apparsa sui vari media, cfr. per tutti: ilgiornale.it del 16 maggio 2010 in http://www.ilgiornale.it e laRepubblica.it del 16 maggio 2010 in http://www.repubblica.it.

[2] A. Antinori, *Information Communication Technology & Crime: the Future of Criminology*, in "Rivista di Criminologia, Vittimologia e Sicurezza", Vol. 21, 2008, n. 3, p. 23 e ss.

taluni la possibilità di infrangere la legge con comportamenti nuovi o modificati dalla tecnologia digitale; uno strumento identificativo tipico di libertà, quale il *web*, è diventato invece fonte di numerosi reati e luogo di privazione della stessa.

Le scienze criminologiche, prendendo atto delle novità comunicative della società, non possono non interessarsi agli aspetti fondamentali della delinquenza che si manifesta attraverso l'uso delle nuove tecnologie informatiche e telematiche.

La rete ha proposto sia nuovi crimini che vecchi reati modificati dalla tecnologia; gli investigatori, dal canto loro, dovranno saper sfruttare queste risorse della tecnologia informatica facendole diventare strumento di indagine e di contrasto del crimine e quindi di ausilio per chi combatte questi delitti, vincendo il silenzio che in genere copre gli abusi di tutti i generi, anche e soprattutto quelli informatici dove la vittima manca di contatto fisico.

Il progresso della criminologia, fondandosi sull'impiego di metodi di ricerca di molte scienze umane, rappresenta una disciplina classicamente applicativa di conoscenze e metodologie provenienti dalla medicina, dal diritto e dalla sociologia, nonché dalla storia e dall'economia. Questa diversità di approcci rende ragione dell'evidenza di multidisciplinarietà della criminologia la quale rappresenta un tradizionale terreno di studio in cui possono trovare legittimità contributi diversi per provenienza e per contenuto, non potendosi delineare una linea interpretativa che sia unitaria ed omogenea.

I contributi si arricchiscono nel momento in cui lo studio criminologico riesce a stare al passo con i tempi, analizzando le più frequenti e socialmente preoccupanti figure di reato. La riflessione sul crimine, sui criminali e la reazione sociale nei confronti dell'illecito sono momenti caratterizzanti la nascita della società e lo svilupparsi della cultura dell'uomo.

Questa diversità culturale ha fatto sì che tutti i criminologi, se pur di diversa estrazione, abbiano apportato il contributo di svariati metodi scientifici con crescita considerevole delle conoscenze reciproche ed accettazione anche delle differenti prospettive.

A seconda dell'affermarsi di nuovi paradigmi interpretativi, ossia delle generali modalità di affrontare e definire il problema dell'uomo di fronte alla norma penale, i contenuti e i metodi della scienza criminologica si sono enormemente evoluti.

Tale atteggiamento ha dunque favorito lo svilupparsi di proposte mirate alla costituzione di un'autonoma ed organica "criminologia interdisciplina-

re", fondata proprio sull'apporto sistematico delle diverse discipline sopra citate.

Attualmente la criminologia sta vivendo un periodo di forte evoluzione grazie ai recenti metodi di rilevamento di tracce, come strumenti tecnici, scientifici, biologici e genetici. Si sta quindi assistendo ad una progressiva enucleazione della materia criminologica, ed alcune tematiche e metodiche sono oggi comunemente fatte rientrare nella cosiddetta "criminalistica": quest'ultima va intesa come quella disciplina volta alla rilevazione di tutti quegli elementi di ordine fisico, chimico, biologico che si connettono con il compimento dell'azione delittuosa.

La "criminalistica" si muove quindi su piani di indagine non sovrapponibili rispetto all'indagine criminologica, tendendo infatti al raggiungimento di obiettivi distinti: la criminologia infatti aspira, a differenza della "criminalistica", alla delineazione del substrato criminogenetico, al fine di comprendere le motivazioni che muovono l'agire e le caratteristiche tipiche del reo. Questi obiettivi, unitariamente allo studio della reazione sociale di fronte al crimine, nonché la individuazione di programmi di difesa sociale, sono appannaggio necessariamente della scienza criminologica la quale, quindi, non può prescindere da un apporto anche socio-psicologico in grado di permettere la comprensione dei costanti cambiamenti che "l'uomo delinquente" compie nell'evoluzione della società.

In un quadro che non può più tornare ad un livello non globalizzato, anche il crimine si pone in un'ottica multimediale e che tende a sfruttare tutte le novità della tecnologia attraverso il missuse e l'abuse.

Ciò significa che la rete degli illeciti ha sfruttato a proprio vantaggio le nuove tecnologie, assorbendo immediatamente la tecnologia in grado di agevolare l'atto contra legem il quale non diventerà una nuova fattispecie di reato, ma sarà un vecchio comportamento deviante con il supporto della tecnologia *on-line*.

Analizzando quindi i reati che maggiormente si sono adeguati alle nuove tecnologie, si osserva che ormai sarà difficile parlare di pedofilia senza analizzarla come fenomeno *on-line*, oppure di apologia di reato senza riscontrare messaggi razzisti o estremisti deliranti provenienti dal *web*, o ancora verificare che in un omicidio il reo e la vittima non abbiano usato il telefono cellulare, *facebook* o le *e-mail*.

In sostanza lo studio del computer crime interessa il criminologo sotto due aspetti: in primis è necessario verificare come la tradizionale figura di reato si sia modificata e si sia adattata alle nuove tecnologie (pedofilia *on-line*,

criminalità organizzata, terrorismo, proselitismo, sette sataniche), successivamente si evidenzia la nascita di nuove figure delittuose emergenti dall'uso delle nuove tecnologie che fondano l'illecito sulle ICT (Cyberpedofilia, *cyber* terrorismo, *hacking*, diffusione di virus informatici, *spamming*, violazione della *privacy*, truffe telematiche via *e-mail*, *netstrike*, *on-line gambling*, diffusione di informazioni illegali *on-line*).

Ulteriore aspetto in un'ottica prettamente procedurale è lo studio della *computer forensic* che riteniamo rientri nell'ambito della "criminalistica"; dal momento che le ICT si caratterizzano per una ingente tracciabilità, queste saranno fonte di prova per gli inquirenti in grado di acquisirla in maniera corretta per successivamente utilizzarla in sede processuale.

Si analizza quindi l'influenza che la tecnologia digitale può avere sulle figure di reato già esistenti e su quelle che diversamente si vengono a creare con l'uso delle ICT.

Il reo, soprattutto quello che il codice penale definisce delinquente professionale o per tendenza e che quindi vive dell'azione delittuosa, si è abituato in maniera istantanea all'uso della tecnologia digitale e delle forme tecnologiche di comunicazione per sfruttarle illecitamente come l'esempio della pedofilia.

Il presente lavoro tenterà di analizzare le *cyber threat*, ovvero il complesso di attività controindicate commesse attraverso le reti e sistemi ICT e/o contro di essi, da una vasta gamma di agenti, i quali, a seconda dei loro attacchi cibernetici, vengono classificati come pedofili, terroristi, estremisti, sabotatori *on-line*.

3. Pedopornografia on-line: la normativa

"Le favole non dicono ai bambini che esistono i draghi,
i bambini già sanno che esistono,
le favole dicono ai bambini che i draghi possono essere uccisi"
Gilbert Keith Chesterton

Esaminando forse il primo comportamento deviante che ha visto l'intrusione dell'uso del computer, ovvero la pedofilia, si nota che già nel 1998 il legislatore aveva ritenuto necessaria l'emanazione di una legge che sanzionasse espressamente i comportamenti di pedopornografia *on-line*.

In realtà non si è trattato della prima volta che nel nostro ordinamento si sono introdotte nuove disposizioni penali per punire condotte illecite realizzate (o realizzabili) per via telematica, infatti già la l. 23 dicembre 1993, n.

547[3], in materia di criminalità informatica, propone un insieme di figure incriminatrici e di norme estensive della punibilità, inserite nel codice penale per punire fatti commissibili anche via rete.

La l. n. 269 del 1998, nota come "legge sulla pedofilia", introducendo nel codice penale gli artt. da 600 *bis* a 600 *septies*, si apre con un vero e proprio preambolo[4] in merito alla tutela dei fanciulli, contro ogni forma di sfruttamento e violenza sessuale a salvaguardia del loro sviluppo fisico, psicologico, spirituale, morale e sociale, costituisce obiettivo primario perseguito dall'Italia[5].

Secondo il titolo della legge, lo sfruttamento della prostituzione, della pornografia e del turismo sessuale in danno ai minori sarebbero «nuove forme di riduzione in schiavitù».

Volendo schematizzare, si può dedurre che il legislatore ha voluto reprimere penalmente certe forme di sfruttamento sessuale ai fini commerciali dei minori considerando l'immaturità sessuale degli stessi. Ha concepito le ipotesi di sfruttamento sessuale dei minori a fini commerciali come nuove forme di riduzione in schiavitù[6], ed ha altresì considerato tali forme di sfruttamento sessuale dei minori a fini commerciali come serie minacce alla salvaguardia dello sviluppo fisico, psicologico, spirituale, morale e sociale[7].

L'art. 3 della l. 269/98 ha introdotto nel corpo del c.p. l'art. 600 *ter* incriminante la pornografia minorile[8]. Sebbene il concetto di pornografia

[3] In G.U. n. 305 del 30 dicembre 1993, "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

[4] Le nuove fattispecie sono state collocate nella Sezione I del Capo III del libro secondo del codice penale, nell'ambito dei "Delitti contro la libertà individuale" ed in particolare dei "Delitti contro la personalità individuale". L'art. 1: "In adesione ai princìpi della Convenzione sui diritti del fanciullo, ratificata ai sensi della l. 27 maggio 1991, n. 176, e a quanto sancito dalla dichiarazione finale della Conferenza mondiale di Stoccolma, adottata il 31 agosto 1996".

[5] A tal fine nella sezione I del capo III del titolo XII del libro secondo del codice penale, dopo l'art. 600 sono inseriti gli artt. da 600 *bis* a 600 *septies*.

[6] A. MANNA (a cura di), *Reati contro la Persona*, Volume II, Torino, Giappicchelli, 2007, *passim*.

[7] A. COLUCCIA, L. LORENZI, M. STRAMBI (a cura di), *Infanzia mal-trattata*, Milano, Franco Angeli, 2002, *passim*.

[8] L'art. 600 *ter*, co. 1 e 2, inserito con l'art. 3 della l. 269/98, recita: "Chiunque sfrutta minori degli anni diciotto al fine di realizzare esibizioni pornografiche o di produrre materiale pornografico è punito con la reclusione da sei a dodici anni e con la multa da lire 25.000 a 250.000. euro. Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma".

non viene definito dal legislatore, gli interpreti hanno cercato di reperire un concetto di pornografia che sia il più chiaro e delineato possibile, dal momento che le sanzioni sono elevatissime.

Solo restringendo la nozione di pornografia a veri e propri atti sessuali del minore, le previsioni di cessione gratuita del materiale pornografico e la semplice detenzione dello stesso da parte del privato, hanno la percezione della illiceità del fatto, cercando di non correre il rischio che foto scattate senza malizia da genitori in vacanza, rientrino potenzialmente tra il materiale di cui è proibito il possesso.

L'art. 600 *ter* c.p. prevede al co. 1 la responsabilità penale di chiunque sfrutti minori degli anni diciotto al fine di realizzare esibizioni pornografiche, di produrre materiale pornografico, e al co. 2 di commerciare detto materiale. I requisiti richiesti dalla norma per la realizzazione della condotta criminosa hanno dato origine a vivaci dispute in dottrina e giurisprudenza[9].

L'orientamento dottrinario prevalente e parte della giurisprudenza richiedono che il fatto sia stato commesso con lo scopo di lucro e con il necessario utilizzo di una struttura imprenditoriale, anche rudimentale: requisito che viene imposto dal termine «sfruttare» utilizzato dal legislatore. Quindi, secondo l'orientamento dottrinario, si esclude l'applicazione di tali norme ad ipotesi in cui il materiale pornografico sia di produzione «casalinga», il risultato di condotte consumate non a scopo di lucro, ma per fini sessuali e con il consenso del minore interessato.

Secondo la giurisprudenza invece, si potrebbero ritenere penalmente rilevanti, ai fini degli artt. 600 *ter* e 600 *quater* c.p. (detenzione di materiale pornografico), anche tutti quei fatti riguardanti materiale pornografico minorile di produzione «casalinga», intendendosi, in generale, per tale produzione quella ottenuta mediante lo sfruttamento di minori degli anni diciotto avvenuto in un contesto non imprenditoriale, ovvero a fini non di lucro.

Anche la distribuzione, la divulgazione ed il pubblicizzare il materiale pornografico posti in essere con qualsiasi mezzo, ivi compreso *Internet*, potranno essere sanzionati, ai sensi dell'art. 600 *ter*, co. 3, altresì quando detto materiale non sia stato ottenuto in un contesto imprenditoriale, o comunque derivi dallo sfruttamento di minori non a scopo di lucro. In particolare, parte della giurisprudenza ha chiarito che per la configurabilità del delitto «è sufficiente che, indipendentemente dalla sussistenza o meno del fine di

[9] Trib. Perugia, Uff. GIP, Sent. 8 luglio 2003, est Micheli; Cass., sez. III, 8 giugno 2006, n. 23164, in "Cassazione penale", 2006, p. 2346; Trib. Lamezia Terme, 4 giugno 2007 n. 252, in "Altalex", 2007.

realizzare esibizioni pornografiche o di produrre il relativo materiale, questo venga propagato ad un numero indeterminato di destinatari»; cosa che può accadere, per esempio, nel caso di cessione a più persone di fotografie pornografiche di minori attraverso l'uso di una *chat-line*[10].

Uno spazio non trascurabile è stato attribuito alla fattispecie in esame, che incrimina in modo esplicito la diffusione di materiale pornografico («anche») via *Internet* («per via telematica»).

La Suprema Corte ha stabilito che, perché sussista divulgazione di materiale pornografico minorile, non è sufficiente che l'autore ceda a singoli soggetti il materiale, ma è necessario che lo propaghi ad un numero indeterminato di persone. La fase di accesso ad una *chat-line*, che riguarda la generalità degli utenti interessati ad un argomento comune, è prodromica rispetto a quella relativa all'individuazione dei partners con cui scambiare messaggi o immagini digitali. La trasmissione di immagini attraverso una *chat-line*, in definitiva, integra, per le modalità con cui viene realizzata, il reato di divulgazione di materiale pornografico minorile.

Il legislatore dopo qualche anno ha ritenuto necessario intervenire nuovamente sul problema pedofilia *on-line*, emanando la l. 6 febbraio 2006 n. 38 "Disposizioni In materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"[11]. Questa legge ha avuto lo scopo di ribadire la necessità di un'azione preventiva delle norme già in vigore e di colmare le lacune ancora esistenti in materia, andando a modificare la normativa vigente, ovvero la l. n. 269 del 1998 ma anche quella sulla violenza sessuale (l. n. 66 del febbraio 1996), dando vigore ai numerosi pronunciamenti a livello europeo per la tutela dei minori contro la pedopornografia effettuata in tutte le modalità, ma soprattutto con il mezzo informatico.

Il legislatore ha cercato di sanzionare la pedofilia virtuale estendendo la pena degli artt. 600 *ter* e 600 *quater* quando il materiale pornografico rap-

[10] L'art. 600 *ter*, co. 3, sancisce: "Chiunque al fuori delle ipotesi di cui al primo e secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga o pubblicizza il materiale pornografico di cui al I comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da 2500 a 50.000 euro. IV comma: Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, consapevolmente cede ad altri, anche a titolo gratuito, materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto, è punito con la reclusione fino a tre anni o con la multa da lire 1500 a 5000 euro".

[11] In G.U. 15 febbraio 2006.

presenta immagini virtuali realizzate utilizzando minori degli anni diciotto o parti di essi, in questo caso la pena è diminuita di un terzo.

Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione li fa apparire come vere immagini. L'intento della nuova legge è quello di arginare il fenomeno ingente della circolazione di materiale pornografico con le reti informatiche ed evitare l'estensione della violenza sessuale nei confronti dei minori ritenendo che queste immagini possano incentivare la molestia ai minori e la pedofilia. Sono stati estesi i limiti di ammissibilità dell'art. 266 del c.p.p. per l'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione per rendere più accessibile la prova nel momento in cui l'intercettato distribuisca, diffonda o pubblicizzi materiale pedopornografico virtuale. Sempre la l. n. 38 ha modificato l'art. 275 c.p.p. in tema di arresto obbligatorio in flagranza di reato per la produzione o il commercio di materiale pedopornografico[12,13].

Dato l'alto grado sanzionatorio della l. n. 38, emergono profili di incostituzionalità sia dal punto di vista dell'indeterminatezza del concetto di pornografia e dei comportamenti riconducibili alla stessa, ma anche per tutti quei casi che si potrebbero definire di pornografia "privata", ovvero quando un minore venga fotografato nudo dal compagno[14].

Inoltre in dottrina c'è chi sostiene che la legge in questione sia troppo sanzionatoria nei confronti dei pedofili dal momento che l'incriminazione "pornografia virtuale" è senza dubbio quella che ha creato le critiche più aspre. Come è stato ben evidenziato si è in presenza di un reato senza vittima in cui è, a dir poco, arduo individuare il bene giuridico oggetto di tutela. In effetti si ha l'impressione che per mezzo di esso il legislatore abbia inteso creare più o meno intenzionalmente nei confronti del pedofilo un clima da "caccia alle streghe" che di certo non si addice ad un sistema penale che si vuole definire moderno: la norma in oggetto arriva a punire il mero pensiero

[12] La Corte costituzionale ha assegnato natura relativa alla presunzione di adeguatezza della misura cautelare in carcere per i reati di cui agli artt. 600 *bis*, co. 1, 609 *bis* e 609 *quater* c.p., introdotta dall'art. 275, co. 3, c.p.p. ad opera del d.l. 23 febbraio 2009, n. 11, conv. con modificazioni, dalla l. 23 aprile 2009, n. 38, in http://www.ipsoa.it/presentazioni/collegati/081090000_DEM.pdf.

[13] *Op. cit. sub* 6.

[14] *Op. cit. sub* 7.

cattivo, in barba al principio *cogitationis poenam nemo patitur*[15].

Il legislatore non ha, ancora, affrontato esplicitamente la questione cruciale dei limiti e dei presupposti della responsabilità penale degli operatori e fornitori di servizi in rete, per i fatti illeciti ivi commessi sia direttamente che da utenti o da terzi. Non ha indicato, né differenziato, i diversi presupposti e titoli di responsabilità in relazione alle specifiche funzioni ed attività svolte. Ora, bisogna rilevare che la dottrina, italiana e non solo, si caratterizza per una impostazione generalmente garantista. La giurisprudenza è apparsa, al contrario, più rigorosa: famoso è rimasto il caso dell'*Internet provider* svizzero che è stato condannato per non aver rimosso materiale pornografico dopo che la presenza di questo gli era stata segnalata dall'Autorità Federale[16].

Ma come può essere ritenuto penalmente responsabile ai sensi dell'art. 600 *ter* l'*Internet provider*? Si potrebbero prefigurare due forme di responsabilità: una di tipo omissivo in base al capoverso dell'art. 40 c.p., e l'altra di tipo commissivo. Secondo la prima ipotesi, si potrebbe sostenere che l'*Internet provider* venga ritenuto responsabile per non aver impedito quell'evento costituito dall'immissione in rete di materiale pedopornografico; l'art. 600 *ter* sembra quindi delineare un delitto di mera condotta con la conseguenza che l'*Internet provider* sarebbe tenuto ad una attività di controllo penalmente sanzionata. Ma è anche vero che alto è il rischio di assegnare all'*Internet provider* un ruolo equivalente a quello di un agente o di un ufficiale di polizia giudiziaria. Un ruolo di controllo che dovrebbe essere del tutto estraneo a chi si limita a svolgere un'attività d'impresa. A tale conclusione, si potrebbe ribattere che nel nostro ordinamento (ed anche in altri), vi sono delle fattispecie in cui vengono prefigurati obblighi di controllo penalmente sanzionati che si ricollegano al ricoprire una carica apicale in complesse strutture organizzative. In tali ipotesi però, è il legislatore che connette doveri di controllo penalmente sanzionati alla titolarità di vertice all'interno di una azienda o di un ente[17].

[15] I. ORMANNI, A. PACCIOLLA, *La pedofilia*, in Palmieri L., "Pediatria forense: Problematiche medico-legali del minore", Padova, Piccin, 2010, p. 735 e ss

[16] Corte di Cassazione Federale Svizzera, 17 febbraio 1995, Rosenberg, in "Enscheidungen des Bundesgerichtshofs", 1995, p. 121.

[17] Cfr. inoltre il par. 14.

3.1. Pedopornografia on-line*: i dati*

La pedopornografia, ovvero qualsiasi rappresentazione di un minore in età prepubere in pose lascive, nudo o impegnato in atti sessuali, ha caratterizzato la fattispecie di pedopornografia *on-line* che consiste in attività di produzione diffusione e commercio in rete Internet di materiale pedopornografico.

La produzione di questo materiale si inserisce in un circuito deviante in grado di sviluppare notevoli proventi economici per le organizzazioni criminali, e questo business si incrementa con le normali leggi economiche della domanda e dell'offerta; purtroppo è evidente che negli ultimi anni la domanda è cresciuta.

La gamma delle immagini pedopornografiche sui bambini va da rappresentazioni nude degli stessi, rapporti sessuali tra loro o con maggiorenni, fino a maltrattamenti che arrivano all'omicidio della vittima. Telefono Arcobaleno ha classificato con una valutazione numerica da 0 a 5, tutte le immagini[18].

Le rappresentazioni degli abusi sessuali sui bambini sono la merce di scambio del pedobusiness e questo materiale circola in rete nei diversi Paesi del mondo perpetuando la memoria dell'abuso fino a quando l'immagine esiste[19].

Attualmente quindi, con l'uso delle tecnologie informatiche, la pedofilia intesa come parafilia[20], prima vissuta in isolamento, è diventata oggi con la facilità degli scambi nella rete, una forma di perversione che coinvolge e aggrega tutta una serie di persone che danno vita ad un ingente giro delinquenziale.

Il computer in definitiva diventa la carta di identità del pedofilo, infatti dal p.c. potremo risalire al materiale che scambia, alle preferenze sessuali, ai contatti che effettua, a verificare le ore del giorno che trascorre *on-line*.

[18] *Content Level Classification*: 0 bambino prepubere non nudo in pose lascive; 1 bambino prepubere nudo senza attività sessuale; 2 bambino prepubere in atti di autoerotismo o attività sessuale non penetrativa tra bambini; 3 attività sessuale non penetrativa tra bambino e adulto; 4 ogni forma di attività sessuale penetrativa che coinvolge bambini con o senza adulti; 5 bambino prepubere in atti di sadismo e crudeltà. Si veda il materiale in .ppt di D. CORSO, *Telefono Arcobaleno Pedofilia on-line. Una nuova forma di violazione dei diritti dell'infanzia*, Catania, 30 maggio 2011.

[19] *Op. cit. sub* 17.

[20] DSM VI, APA, Diagnostic and Statistical Manual of Mental Disorders, DSM IV –TR, 2000.

Le reti in uso al pedofilo *on-line* sono in genere le stesse che si usano per motivi meno abietti, quindi si può reperire materiale pedopornografico in normali siti *web*, con iscrizione o a pagamento, aperti a tutti oppure a una fascia di persone predefinite in *Discussion Board* o Bacheche per scambi di *link* e informazioni. Più spesso però usano *On-line storage*, o attività di interscambio di materiali illegali attraverso servizi di storage *hard disk* virtuali che hanno funzioni di archivio *on-line* e, in genere, questi materiali sono protetti da *password*.

Inoltre usano il sistema *Peer to Peer* (*e-mule*) per attività di condivisione e scambio di materiali pedofili, interconnessioni degli utenti fra loro senza attività di intermediazione e anche *Chat* e *Social Network*.

Il materiale può essere di produzione amatoriale o più frequentemente di produzione professionale.

L'offerta pedopornografica sul *web* è strutturata e organizzata secondo le più comuni regole del marketing: dai siti pedo promozionali, livelli più visibili e superficiali della rete, fino ai siti a pagamento che occupano i livelli meno conosciuti e raggiungibili della rete.

I pagamenti avvengono attraverso transazioni *on-line* gestite da siti Internet molto volatili, per lo più allocati presso *server* statunitensi, olandesi, russi, ucraini e tedeschi, e si avvantaggiano dell'uso delle più comuni carte di credito. Talvolta usano delle vere e proprie forme di abbonamento, ovvero il cliente riceve una password attraverso la quale può avere accesso a contenuti pedopornografici sempre nuovi per un certo periodo di tempo[21].

I dati inerenti il fenomeno della pedopornografia *on-line* sono veramente sconvolgenti; dall'attività di monitoraggio e *hunting* di Telefono Arcobaleno emerge che i siti pedofili segnalati nell'anno 2010 sono risultati essere 52.373; il loro numero progressivo dal 1996 è di 361.364, con una performance di chiusura degli stessi del 99,2%.

Nei soli primi 5 mesi del 2011 le segnalazioni sono risultate essere 32.837.

L'età delle vittime segnalate nel 2010 sono:

- 5,3% da 0 a 1 anno;
- 6,7% da 2 a 3 anni;
- 30,5% da 4 a 6 anni;
- 36,4%, da 7 a 10 anni;
- 21,1% dagli 11 ai 14 anni.

[21] International Observatory Against Child Abuse and Sexual Exploitation, Short Report, 2011, Aprile (centrostudi@telefonoarcobaleno.org)

Inquietante il dato dell'età dei minori abusati su materiale pedopornografico dei primi 5 mesi del 2011 che è risultato essere del 38% da 0 a 5 anni, suddivisi in 30% da 3 a 5 anni, 7% da 0 a 3 anni e un 1% di neonati.

Anche l'offerta del materiale pedopornografico *on-line* è cambiato nel giro di pochi anni; i dati dell'attività di *hunting* di telefono Arcobaleno dimostrano che se nel 2007 il maggior offerente di materiale era la Germania con il 65%, seguita dall'8% degli USA e l'11% dei Paesi Bassi, (più un 15% di tutti gli altri Paesi) attualmente vediamo che nei primi 3 mesi del 2011 la percentuale dei Paesi offerenti materiale pedopornografico del 79% si concentra nei seguenti Stati:

- 42% USA
- 14,6 Paesi Bassi
- 11% Germania
- 10,6 Federazione Russa

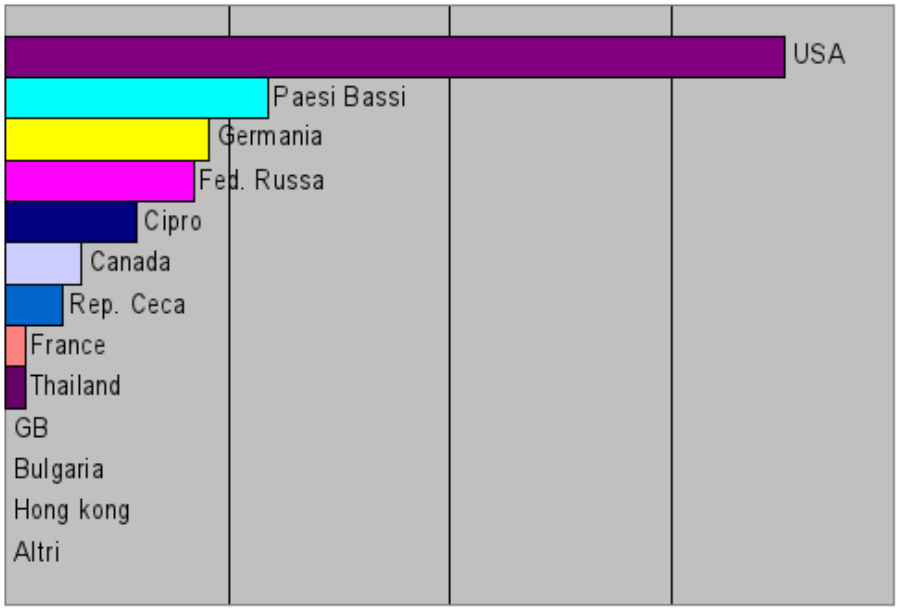

Fig. 1 – Offerta mondiale pedofilia on-line

Diversamente, la domanda di materiale pedopornografico *on-line* vede il 52% della richiesta nei seguenti Paesi:

- 23% USA

- 17% Germania
- 6% Federazione Russa
- 5,6% Italia

I dati dimostrano che sebbene l'Italia non sia un Paese produttore di materiale pedopornografico *on-line*, si pone al quarto posto come domanda dello stesso.

Secondo l'Associazione Meter[22] sono quasi 70.000, precisamente 69.850 il numero dei minori conteggiati uno per uno nel Report annuale 2010 durante il monitoraggio della rete Internet e nelle segnalazioni dei siti pedopornografici. Sono 689.394 i siti monitorati dal 2003 al 2010. Di questi, 65.056 sono stati segnalati alle Polizie di tutto il mondo e in particolare alla Polizia Postale e delle Comunicazioni italiana per i contenuti pedofili e pedopornografici. Nel 2010 sono 13.766 i siti con contenuto pedofilo (7.240 nel 2009).

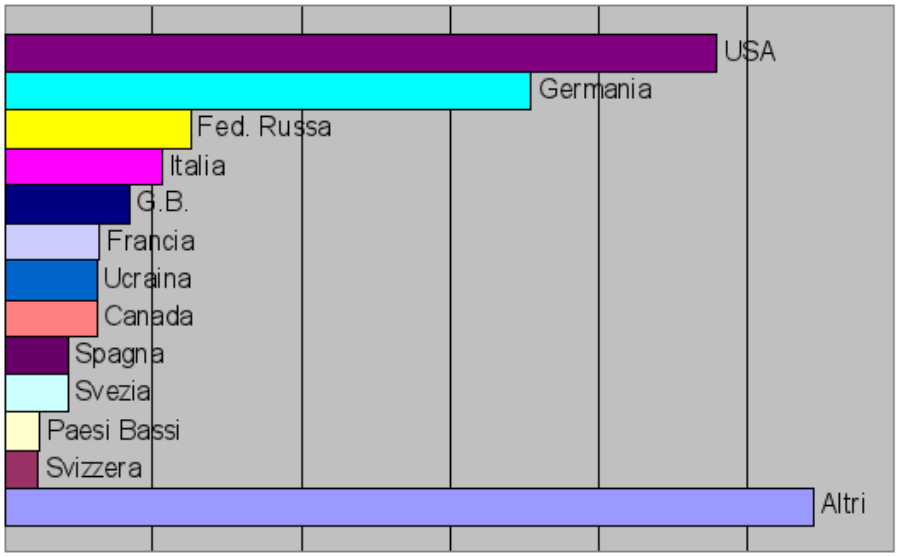

Fig. 2 – Domanda mondiale pedofilia on-line

22 http://www.pontifex.roma.it/index.php/opinioni/consacrati/8656-associazione-meter-onlus-del-caro-don-fortunato-di-noto-pioniere-nella-lotta-antipedofilia.

3.2. Pedopornografia on-line*: aspetti di* criminal profiling

In Italia, attraverso il progetto O.L.D.PE.PSY.[23] (*On Line Detected Pedophilia Psychology*) gli studiosi cercano di contribuire alla prevenzione e repressione del fenomeno pedopornografico analizzando il ruolo che svolge Internet nell'ambito della pedofilia e qual è il rischio reale che un minore possa essere molestato *on-line*. Soprattutto si cerca di analizzare il *modus operandi* del pedofilo *on-line* e se questa attività è sostitutiva, parallela o incentivante dell'abuso fisico.

L'esperienza degli agenti sotto copertura ha permesso di delineare alcune tipologie cliniche e psicologiche di pedofili *on-line*, evidenziando comunque una casistica disomogenea di approccio con il minore che variano da semplici fantasie intrapsichiche (non agite) a forme di contatto fisico saltuario o stabile fino a giungere a contatti violenti correlati talvolta all'omicidio della giovane vittima[24].

La classificazione del prof. Strano rappresenta una prima definizione tassonomica del tipico comportamento pedofilo riscontrato via Internet:

1. Un comportamento pedofilo "voyeuristico", centrato sulla fruizione di materiale pedopornografico (attività esclusiva), senza un contatto fisico con i minori. Tale categoria comprende la prevalenza dei soggetti studiati (circa l'89% del campione).
2. Un comportamento pedofilo "misto", caratterizzato da fruizione sistematica di materiale pedopornografico (attività prevalente) e da rari occasionali contatti con minori (intrafamiliari o con minori avvicinati casualmente). Tale categoria comprende una ridotta percentuale di soggetti (circa l'8% del campione)
3. Un comportamento pedofilo "misto", caratterizzato da fruizione sistematica di materiale pedopornografico e comprendente frequenti e reiterati contatti fisici con minori (intrafamiliari o nel corso di incontri "cercati" con bambini conosciuti e avvicinati dal soggetto). Tale categoria comprende apparentemente una minima percentuale del campione (circa il 2%).
4. Un comportamento pedofilo centrato sull'abuso fisico di minori, ricercato attraverso la prostituzione minorile e il "turismo sessuale".

[23] M. STRANO, *Manuale di criminologia clinica*, Firenze, SEE, 2003, p. 375 e ss.

[24] M. STRANO, *Uno studio clinico e criminologico dei pedofili on-line*, Relazione al Congresso Internazionale della Società Italiana di Psicopatologia – SOPSI (Roma, Hotel Hilton, 26 febbraio 2003).

"articoli/devivo" — 2012/4/5 — 10:45 — page 42 — #42

In tale quadro la pedopornografia rappresenta un fattore di contorno. Tale categoria comprende una piccolissima percentuale del campione (circa l'1%).

La tipologia proposta si basa sulle informazioni che sono state acquisite nel corso delle indagini. Non si può escludere che alcuni dei soggetti apparentemente solo fruitori di materiale pedopornografico (senza apparenti contatti fisici con minori) possano in realtà aver commesso abusi fisici non evidenziati dall'attività investigativa[25].

La l. n. 38 del 2006 ha previsto inoltre la costituzione di due nuovi organismi: il primo, denominato "Centro nazionale per il contrasto della pedopornografia sulla rete Internet", istituito presso il Ministero dell'Interno e ha il compito di raccogliere le segnalazioni provenienti da soggetti pubblici e privati, relative ai siti che diffondono materiale concernente l'utilizzo sessuale dei minori avvalendosi di Internet. In questo centro sono elencati tutti i siti segnalati e aggiornati costantemente con i nominativi dei gestori e dei beneficiari dei relativi pagamenti.

Sulla base dei dati in suo possesso, il Centro comunica ad un altro organismo, l' "Osservatorio per il contrasto della pedofilia e della pedopornografica minorile", gli elementi informativi e i dati statistici relativi alla pedopornografia in rete al fine di predisporre un Piano nazionale di contrasto e prevenzione della pedofilia e una relazione annuale. Anche presso l'Osservatorio in questione è prevista l'istituzione di una banca dati, contenente tutte le informazioni utili per il monitoraggio del fenomeno.

4. I REATI COMMESSI CON L'USO DEL PC: IL CYBER TERRORISMO

"Ogni società ha il tipo di criminali che si merita"
Robert Kennedy

Negli anni '70 Internet si sviluppa negli Stati Uniti, durante i giorni della guerra fredda, quando il Dipartimento della Difesa era intento a ridurre la vulnerabilità delle sue reti di comunicazione da un eventuale attacco nucleare; conseguentemente il Pentagono cercò di decentrare l'intero sistema di difesa con la creazione di una rete interconnessa di computer.

Se ai tempi della guerra fredda la minaccia "totale" era rappresentata dall'arma nucleare, cioè dall'uso a fini di distruzione di massa dell'energia nu-

[25] *Op. cit. sub* 22.

cleare, oggi, in tempi di competizione globale, l'"arma totale" è rappresentata dall'uso offensivo degli strumenti dell'informatica e della telematica[26].

Appare evidente che, sebbene la rete incarni gli ideali di democrazia e libertà, taluni non hanno esitato a strumentalizzarla, deviandola dal lecito ed andando ad abusare della sua grande libertà di comunicazione, rendendo necessari controlli e censure, demolendo i suoi ideali iniziali e contrastando con il libero pensiero. Per soggetti già *border line*, il facile accesso alla rete, lo scarso controllo, l'assente censura, l'enormità del pubblico in tutto il mondo, l'ambiente multimediale, ma soprattutto l'anonimato di chi comunica, hanno fatto sì che Internet potesse diventare una loro arena ideale per fini illeciti quali terrorismo, eversione, apologia ecc.

L'enorme crescita dell'uso della rete ha visto inevitabilmente sorgere siti pedopornografici, violenti, eversivi, usati da organizzazioni estremiste di tutti i tipi, ma con il comune intento di diffondere la loro propaganda, il terrore e l'uso della violenza; Islamists and Marxists, nationalists and separatists, racists and anarchists: all find the Internet alluring.islamisti e marxisti, nazionalisti e separatisti, razzisti e anarchici: tutte queste categorie si possono trovare in Internet propagandare le loro idee[27].

Tutto ciò sinora prospettato denota complessi devianti che possono essere definiti "minacce cibernetiche" o *cyber threat*, attuate dagli attori più svariati che, sebbene si riferiscano al mondo intangibile del *cyber space*, rappresentano aspetti estremamente tangibili e socialmente pericolosi.

[26] G. DE GENNARO, *La minaccia cibernetica*, Formiche, febbraio 2011, in http://www.formiche.net/dettaglio.asp?id=26455&id_sezione=79.

[27] Dal Medio Oriente, Hamas (il Movimento di Resistenza Islamico), il libanese Hezbollah (Partito di Dio), le Brigate Martiri di al Aqsa, Tanzim di Fatah, il Fronte Popolare per la Liberazione della Palestina (FPLP), la Jihad islamica palestinese, il Kahane Movimento vive, Mujahidin del Popolo Iraniano (PMOI-Mujahidin-e Khalq), Party (PKK) dei Lavoratori del Kurdistan, e il turco a base di Popolare Partito democratico Fronte di Liberazione (DHKP / C) e Grande Oriente del Fronte islamico di Raiders (IBDA- C). Dall'Europa, il movimento basco ETA, Armata Corsa (l'Esercito della Corsica), e l'Esercito Repubblicano Irlandese (IRA). Dall'America Latina, Perù Tupak-Amaru (MRTA) e di Sendero Luminoso (Sendero Luminoso), il colombiano Esercito di Liberazione Nazionale (ELN-Colombia) e le Forze Armate Rivoluzionarie della Colombia (FARC). Dall'Asia, al Qaeda, la Verità Suprema giapponese (Aum Shinrikyo), Ansar al Islam (Sostenitori dell'Islam) in Iraq, l'Armata Rossa Giapponese (JRA), Hizb-ul Mujehideen in Kashmir, le Tigri di Liberazione del Tamil Eelam (LTTE), il Movimento Islamico dell'Uzbekistan (IMU), il Moro Islamic Liberation Front (MILF), nelle Filippine, il Pakistan a base Lashkare-Taiba e il movimento ribelle in Cecenia. In proposito si rinvia alla consultazione di G. WEIMANN, *How Modern Terrorism Uses the Internet*, Report dell'Institute of Peace of United States, in http://www.usip.org/files/resources/sr116.pdf.

Il terrorismo informatico si può definire come l'utilizzo di tecnologie informatiche (computer, *network* informatici, *software*, ecc.) al fine di procurare un vantaggio in un'azione o strategia terroristica[28,29].

4.1. Terrorismo e cyber *terrorismo*

Il *cyber* terrorismo può essere considerato un sottoinsieme della più ampia categoria detta *Info War* o *Information Warfare*. L'*Info War* è caratterizzata dallo studio di metodologie di attacco o difesa di strutture di gestione delle informazioni, ed il suo fine è quello di provocare, a seconda degli obiettivi specifici, la protezione o distruzione di informazioni sensibili in relazione al contesto in cui si opera[30].

Il nostro Paese ha visto espressioni terroristiche di diversi tipi: il terrorismo a vocazione nazionalista e indipendentista, il terrorismo estremista rivoluzionario ed il terrorismo internazionale.

Attualmente anche l'Italia ha sviluppato una tutela sia nei confronti del terrorismo interno, sia verso i potenziali attacchi del *cyber* terrorismo, grazie agli studi di *information security*. Al momento il panorama che si delinea, e non solo a livello regionale, è di due tipi:

1. terroristi che usano la rete per diffondere, potenziare, reclutare ed inneggiare alle più svariate forme eversive terroristiche;
2. terroristi che portano quasi esclusivamente attacchi informatici e *cyberwarfare* con finalità terroristiche[31,32].

In merito alla prima forma di terrorismo *on-line*, si rinvengono fenomeni quali il reclutamento di terroristi per fini eversivi, esaltazione di fazioni estremiste politiche e religiose, inneggiamento a stragi di massa per motivi razziali, fenomeni satanisti.

[28] D.S. PUTIGNANO, *Il Cyberterrorismo e la normativa italiana*, in http://www.studioputignano.it/diritto-penale-pubblicazione.htm

[29] V. MUSACCHIO, *Internet and International Terrorism: A Dangerous Assosiation*, in "Ciberspazio e Diritto", Vol. 6, 2005, n. 3, pp. 415-422; G. ZICCARDI, *Informatica Giuridica*, II, Milano, Giuffrè, 2008, *passim*; *M. Strano, B. Negre, P. Galdieri*, *Cyberterrorismo. L'impiego delle reti telematiche da parte del terrorismo internazionale*, Milano, Jackson Libri, 2002, *passim*.

[30] G. ZICCARDI, *Manuale breve di informatica giuridica*, Milano, Giuffrè, 2008, *passim*.

[31] *Op. cit.*, *sub* 26.

[32] D. FRANKLIN, H. KRAMER, S. STUART, L.K. WENTZ, *Cyberpower and National Security*, Dulles, Potomac Books Inc, 30/apr/2009; D. VERTON, *Black Ice: The Invisible Threat of Cyber-war*, McGraw-Hill, 2003.

Il secondo tipo, ovvero il *cyber* terrorismo, è forse di natura più sofisticata e si concentra verso gli obiettivi sensibili dei singoli Stati; si avvale della volatilità dei siti *web* ed è facilitato dall'alta decentralizzazione delle tecnologie informatiche. Le sue conseguenze, se poste in atto, possono essere devastanti.

Già nel 2004 negli USA, il rapporto tra terrorismo ed uso di Internet era evidente, infatti nel dettagliato resoconto dello *United States Institute of Peace*, dal titolo "How modern terrorism uses the Internet", e redatto nel 2004 da Weimann[33], sono descritte tutte le modalità con cui si manifesta questo legame tra Internet e il mondo del terrorismo.

Il rapporto Weiman ha analizzato centinaia di siti con finalità terroristiche ed è emerso che, generalmente, c'è una forma standard per i contenuti dei siti in questione; in essi è presente la storia dell'organizzazione, le attività svolte, i punti ideologici fondamentali, il luogo di azione o dove vorrebbero agire, le biografie dei leader del gruppo e soprattutto i proclami contro gli avversari politici e l'esaltazione dei loro propositi eversivi.

Weiman[34] suddivide in tre direzioni la tipologia del destinatario del messaggio eversivo, talché il primo è rivolto a sostenitori attuali e potenziali, il secondo è di natura internazionale per coinvolgere più soggetti possibile e il terzo è inviato agli avversari con proclami di annientamento, minacce ed autoesaltazione. Il terrorismo è stato spesso concepito come una forma di guerra psicologica, e per attuarla i terroristi usano diverse metodologie come instillare paure e minacce, mostrare immagini brutali ed omicidi e, solo di recente, instillare il timore del *cyber* terrorismo.

Cosa diversa è la *cyberfear* che si concretizza nella sociale preoccupazione per quello che un attacco informatico potrebbe fare (es. abbattere aerei disabilitando sistemi di controllo del traffico, o distruggere le economie nazionali eliminando i sistemi informatici che regolano i mercati azionari) e si ingrandisce fino a quando l'opinione pubblica ritiene che un attacco "accadrà", amplificando il suo messaggio ed esagerando l'importanza e la minaccia che rappresenta[35].

I siti terroristici per giustificare l'uso della violenza adottano una "struttura retorica" del tutto peculiare, ovvero affermano che non hanno alcuna alternativa all'uso della violenza, la quale è la sola possibilità per i deboli di

[33] *Op. cit.*, *sub* 26.
[34] *Op. cit.*, *sub* 26.
[35] *Op. cit.*, *sub* 26.

fronteggiare un nemico oppressivo; inoltre si rappresentano come vittime e perseguitati che lottano per la libertà. Oltre a ciò affermano la legittimità della violenza per demonizzare e delegittimare il nemico, dichiarando che il vero avversario è quello contrario al loro movimento e accusandolo di brutalità e disumanità.

Il modo di espressione che accomuna i siti terroristici è una caratteristica imprescindibile per catturare l'attenzione di soggetti sprovveduti, infatti il linguaggio si avvale di idiomi e lessici tipici della non violenza, nel tentativo di contrastare la loro immagine aggressiva, dando l'idea di essere coloro che cercano di trovare soluzioni pacifiche e diplomatiche attraverso la pressione internazionale ed il negoziato, diversamente dalle Autorità governative che hanno un atteggiamento repressivo e non collaborativo[36].

Un'altra caratteristica assai peculiare per il terrorismo *on-line* è il *fundraising*, ovvero l'uso di Internet per la raccolta fondi destinati allo scopo illecito attraverso donazioni che i soggetti possono effettuare direttamente *on-line* con carte di credito[37].

Naturalmente questo è un punto estremamente importante per il sostentamento delle organizzazioni eversive e terroristiche e per la loro dislocazione territoriale; sarebbe estremamente difficile ricevere donazioni economiche attraverso circuiti leciti.

In tema di circuiti finanziari e con specifico riferimento a canali di trasferimento di valuta che potrebbero essere sfruttati per finalità illecite incluso il finanziamento di organizzazioni terroristiche, si conferma la crescente ri-

[36] *Op. cit.*, *sub* 26.

[37] Il gruppo estremista sunnita Hizb al-Tahrir utilizza una rete integrata di siti Internet, che si estende dall'Europa all'Africa, che chiede sostenitori per aiutare lo sforzo dando soldi e incoraggiando gli altri a donare alla causa della jihad. Le informazioni bancarie sono fornite da un sito con sede in Germania, compresi i numeri di conti in cui le donazioni possono essere depositate. I combattenti nella repubblica secessionista russa della Cecenia hanno anche usato Internet per pubblicizzare il numero di conti bancari a cui i simpatizzanti possono contribuire. Uno di questi conti bancari ceceno si trova a Sacramento, in California. Il sito dell'IRA contiene una pagina in cui i visitatori possono fare donazioni con carta di credito. Nel gennaio 2004, un gran giurì federale dell' Idaho condannò uno studente laureato in Arabo per aver contribuito ad aiutare le organizzazioni terroristiche jihad, utilizzando Internet per raccogliere fondi, reclutare ed individuare potenziali obiettivi statunitensi, militari e civili, nel Medio Oriente. Omar Hussayen, un candidato al dottorato in informatica in una Università dell'Idaho, con un programma sponsorizzato dalla *National Security Agency*, è stato accusato di creare siti *web* e una *e-mail* per supportare la *jihad*, in http://www.difesa.it/SMD/CASD/Istituti_militari/CeMISS/Pubblicazioni/OsservatorioStrategico/Documents/98135_oss_sett04.pdf.

levanza di sistemi alternativi di trasferimento fondi quali quelli denominati *hawala* e *euro to euro*. Il sistema *hawala* (in arabo ordine di pagamento) è un circuito bancario parallelo che consente il trasferimento di denaro senza comportarne la movimentazione fisica, si basa sul versamento di somme ad intermediari che garantiscono la consegna di un equivalente importo in valuta locale nel paese di destinazione; il sistema *euro to euro*, utilizzato in particolare dalla comunità nigeriana, si sviluppa attraverso una rete di raccolta del contante in esercizi commerciali nel nostro paese e a questi corrisponde un ufficio nel paese estero presso il quale le somme "affidate" in Italia possono essere incassate sul posto dopo ventiquattro ore[38].

Infine ciò che praticamente agevola le organizzazioni terroristiche ed eversive sono i contatti che si possono instaurare e mantenere tramite i *network* e la possibilità di condivisione delle informazioni, tenendo contatti tra i vari gruppi ed avendo un'organizzazione decentrata con un coordinamento orizzontale anziché verticale, riducendo sia i tempi di trasmissione che i costi di comunicazione, ma anche la possibilità di aumentare notevolmente la complessità delle informazioni che possono essere condivise[39].

[38] PRESIDENZA DEL CONSIGLIO DEI MINISTRI, *Sistema di informazione per la sicurezza della repubblica, Relazione sulla politica dell'informazione per la sicurezza*, 2010, in http://www.sicurezzanazionale.gov.it/web.nsf/relazione2010/relazione_2010.pdf.

[39] Il World Wide Web è la patria di decine di siti che forniscono informazioni su come costruire armi chimiche ed esplosivi. Molti di questi siti, dopo il "Manuale del terrorista" e *The Anarchist Cookbook*, due noti manuali, offrono istruzioni dettagliate su come costruire una vasta gamma di bombe. Un altro manuale, Il Manuale Mujahadeen dei veleni, scritto da Abdel-Aziz nel 1996 e "pubblicato" sul sito ufficiale di Hamas, contiene i dettagli in 23 pagine su come preparare vari veleni fatti in casa, gas velenosi, mortali e altri materiali per l'uso in attacchi terroristici. Un manuale molto più grande, soprannominato "L'Enciclopedia della Jihad" e preparato da al Qaeda, coinvolge migliaia di pagine. Questi manuali, distribuiti attraverso Internet, offrono istruzioni dettagliate su come stabilire una organizzazione clandestina ed eseguire attacchi. Queste informazioni vengono visionate non solo da sofisticate organizzazioni terroristiche, ma anche da individui *border line* pronti ad usare tattiche terroristiche per sviluppare il proprio programma idiosincratico. Nel 1999, un giovane di nome David Copeland fabbricò bombe chiodate e le fece saltare in tre diverse aree di Londra: nella zona multirazziale di Brixton, nella comunità Bangladesh di Brick Lane, e nel quartiere gay di Soho. Al suo processo, ha rivelato di aver appreso le sue tecniche letali da Internet, il cui download era dal manuale del terrorista e ESTONIAESTONIA. Entrambi i titoli sono ancora facilmente accessibili. Una ricerca attraverso le parole chiave "terrorista" e "manuale" sul motore di ricerca Google ha trovato quasi 4000 risultati con riferimenti a guide e manuali. Servizio per le l'informazione e la sicurezza democratica, in *Rivista italiana di Intelligence*, XIII, 1, 2007, http://www.bv.ipzs.it/bv-pdf/004/MOD-BP-06-5-4_67_1.pdf.

4.2. Normativa antiterrorismo

L'FBI inquadra il terrorismo entro due categorie generali: uno interno e l'altro internazionale. Il terrorismo interno è definito come "l'uso illegale, o minacciato, della violenza da parte di un gruppo o di un individuo la cui base si trova esclusivamente all'interno degli Stati Uniti o nei loro territori, senza direzione dall'estero, e avente di mira persone o proprietà con intento di intimorire o di coartare governo o popolazione al fine di conseguire obiettivi politici o sociali"[40].

Il terrorismo internazionale invece comprende "atti violenti, o pericolosi per la vita umana, che violano le leggi criminali degli Stati Uniti o di altri Stati, o che sarebbero una violazione criminale se commessi entro la giurisdizione degli Stati Uniti o di altri Stati, e miranti ad intimorire o coartare la popolazione civile, influenzare la politica governativa, o influire sul comportamento di un governo"[41].

La definizione italiana di terrorismo possiamo mutuarla dall'art. 270 *bis* c.p. che punisce chiunque promuove, costituisce, organizza, dirige, finanzia o partecipa ad associazioni che si propongono di compiere "atti di violenza con finalità di terrorismo", anche rivolti contro uno Stato estero o un'istituzione internazionale.

Successivamente il d.l. 144 del 2005[42] ha introdotto l'art. 270 *sexies* recependo fedelmente la decisione quadro dell'UE 2002/475/GAI in cui si considerano con finalità di terrorismo le "condotte che, per la loro natura o contesto, possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici (...) a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture (...) di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche (...) da (...) norme di diritto internazionale vincolanti per l'Italia".

La Decisione quadro riduce la sfera di applicazione ai fatti commessi in tempo di pace, escludendo le attività delle Forze Armate in tempo di conflitto armato, regolate dal diritto internazionale.

[40] D. PERLMUTTER, *Satanisti e terroristi*, in "Anthropoetics 7", 2001-2002, n. 2.

[41] D. PERLMUTTER, *Op. cit.*, *sub* 40.

[42] Cfr. d.l. 27 luglio 2005, n. 144 "Misure urgenti per il contrasto del terrorismo internazionale", in G.U. 173 del 27 luglio 2005, convertito in l. 31 luglio 2005, n. 155, in G.U. n. 177 del 1 agosto 2005.

L'art. 270 *sexies* c.p. richiede che la finalità di terrorismo vada rilevata dalla natura e contesto delle condotte, e necessita di un grave danno, sebbene questi requisiti non siano presenti nell'art. 270 *bis* c.p. che però richiede la natura violenta delle condotte, elemento non presente nell'art. 270 *sexies* c.p.[43]; da ciò emerge che i due articoli formano un combinato disposto in quanto non tutti gli atti violenti creano un grave danno, così come l'elemento della violenza non è l'unico a cagionare un grave danno, soprattutto nel caso di attacchi informatici.

Le fattispecie in esame rientrano tra i reati a pericolo presunto e l'oggetto di tutela penale prevede due forme di garanzia, uno a tutela alla personalità dello Stato, l'altro a tutela dell'ordine pubblico, elementi entrambi lesi per effetto della violenza[44].

È una fattispecie delittuosa che prevede una pluralità di persone, legate da un vincolo in una struttura transnazionale, dotata di mezzi idonei per raggiungere lo scopo a commettere atti terroristici. La dottrina maggioritaria contempla l'elemento soggettivo del dolo specifico, ma la giurisprudenza accoglie la tesi del dolo generico di partecipazione all'associazione deviante. Il tentativo è escluso poiché gli atti diretti sarebbero già sufficientemente eloquenti per la costituzione di un'associazione terroristica, ma altra parte della dottrina lo ritiene configurabile qualora gli atti non arrivino alla sua attuazione.

L'art. 270 *quater* sanziona chi arruola una o più persone per il compimento di atti terroristici, ma non è prevista pena per i reclutati.

La lotta al finanziamento delle associazioni terroristiche è il punto fondamentale della normativa per colpire in maniera fattiva tali gruppi, infatti la nostra legislazione ha previsto, accanto alle misure di carattere penale, quelle patrimoniali che hanno lo scopo di aggredire le risorse ed i finanziamenti diretti ad organizzazioni terroristiche, ed anche la misura cautelare del congelamento dei fondi e delle risorse per queste finalità; questo strumento

[43] M.T. TONDINI, J.P. PIERINI, *Tavole di legislazione e giurisprudenza comparata sul fenomeno del terrorismo internazionale*, Luglio 2007, in http://www.forumcostituzionale.it/site/images/stories/pdf/nuovi%20pdf/Paper/0049_tondini-pierini.pdf; L.D. CERQUA, *La nozione di "condotte con finalità di terrorismo" secondo le fonti internazionali e la normativa italiana*, in "Revista Brasileira de Estudos Políticos", in http://www.pos.direito.ufmg.br/rbep/096031114.pdf.

[44] http://dspace-unipr.cilea.it/bitstream/1889/923/1/i_delitti_contro_la_personalit%C3%A0_dello_Stato.pdf.

appare il mezzo più idoneo allo scopo. Nella l. 14 dicembre 2001, n. 431[45] recante misure urgenti per reprimere e contrastare il finanziamento del terrorismo internazionale, è stato istituito presso il Ministero dell'Economia e delle Finanze, il Comitato di Sicurezza Finanziaria (CSF)[46]. Al CSF compete sia l'attuazione delle misure di congelamento adottate dall'Unione Europea nei confronti delle disponibilità economiche e finanziarie delle organizzazioni terroristiche, sia l'applicazione delle sanzioni previste nei confronti degli intermediari.

Passando all'analisi del reato di *cyber* terrorismo, si nota che solitamente il terrorista accede all'interno di un sistema altrui, di conseguenza è l'art. 615 *ter* c.p. la fattispecie inquisitoria così come modificato dalla l. n. 48 del 2008[47], che sanziona l'accesso abusivo all'interno di un sistema informatico o telematico. Tutela maggiormente incisiva è riservata proprio a quei sistemi che, più degli altri, possono costituire un obiettivo del *cyber* terrorista, ovvero quelli di interesse militare o relativi all'ordine e alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse dello Stato.

Sovente l'attacco informatico si realizza attraverso l'immissione nel sistema dei cosiddetti virus informatici, e per far fronte a tali pericoli è stato introdotto nel nostro Paese l'art. 615 *quinquies* c.p. che sanziona la diffusione di programmi informatici volti al danneggiamento di sistemi o di programmi e dati in essi contenuti.

Altre norme che consentono di punire condotte realizzabili anche dai gruppi terroristici sono gli artt. 617 *quater* - 617 *sexies* c.p. riguardanti le intercettazioni informatiche e telematiche. Il primo punisce tanto la condotta

[45] Cfr. l. 14 dicembre 2001, n. 431 "Conversione in legge, con modificazioni, del d.l. 12 ottobre 2001, n. 369, recante misure urgenti per reprimere e contrastare il finanziamento del terrorismo internazionale" in G.U. n. 290 del 14 dicembre 2001.

[46] Il Comitato è presieduto dal Direttore Generale del Tesoro e si compone di 11 membri nominati dal Ministro dell'Economia e delle Finanze sulla base delle designazioni operate dai Ministri dell'Interno, della Giustizia, degli Affari Esteri, dalla Banca d'Italia, dalla Commissione Nazionale per le Società e la Borsa (CONSOB) e dall'Ufficio Italiano Cambi (UIC). Del Comitato fanno parte un dirigente del Ministero dell'Economia e Finanze, un Ufficiale della Guardia di Finanza, un ufficiale/funzionario della Direzione Investigativa Antimafia (DIA), un Ufficiale dell'Arma dei Carabinieri ed un rappresentante della Direzionale Nazionale Antimafia. http://www.dt.tesoro.it/it/prevenzione_reati_finanziari/comitato_sicurezza_finanziaria/

[47] Cfr. l. 18 marzo 2008, n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno" in G.U. n. 80 del 4 aprile 2008 - Supplemento ordinario n. 79.

di chi intercetta, impedisce o interrompe comunicazioni relative a un sistema o fra più sistemi, sia quella di chi rivela al pubblico il contenuto delle informazioni. Con l'art. 617 *quater* si punisce la ricezione comunque avvenuta, con l'art. 617 *quinquies* si colpisce l'organizzazione voluta e predisposta per quel fine e la fattispecie dell'art. 617 sexies consente di punire la falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche[48].

4.3. Possibili conseguenze del cyber *terrorismo*

A Lisbona nel vertice NATO del novembre 2010 il nuovo concetto strategico adottato da tutti i Capi di Stato dei Paesi membri è stato quello di potenziare la capacità di prevenire, individuare difendersi e riprendersi da attacchi informatici ritenuti potenzialmente in grado di minacciare la prosperità, la sicurezza e la stabilità nazionale ed euro atlantica.

L'aumentata consapevolezza a livello globale delle potenzialità e dei rischi della rete informatica si è accompagnata alla diffusa percezione dello spazio cibernetico quale possibile campo di battaglia. Il *cyber space* è sempre più considerato – dopo terra, mare, cielo e spazio – il quinto dominio della "difesa militare"[49] proprio a causa della dipendenza informatica dei Paesi tecnologicamente più avanzati.

In Italia in merito alla tutela nazionale si possono ricordare le raccomandazioni del Comitato Parlamentare per la sicurezza della Repubblica, che hanno sottolineato la necessità di una pianificazione a livello nazionale e di un impianto organizzativo che assicuri il coordinamento tra gli attori interessati "anche attraverso la ridefinizione delle attività delle strutture esistenti ed una rimodulazione delle attuali competenze e responsabilità"[50].

Esistono una serie di postazioni strategiche, definite infrastrutture critiche, che si caratterizzano per essere il punto nevralgico per il funzionamento organizzativo di uno Stato, ovvero quell'insieme di infrastrutture che garantiscono il benessere sociale ed economico di una nazione.

[48] *Op. cit.*, *sub* 27.

[49] Il ruolo dell'Autorità Nazionale per la Sicurezza nell'ambito della *Cyber security*, Rapporto nazionale 2010, http://w3.uniroma1.it/mastersicurezza/images/materiali/Convegni/ANS.pdf.

[50] *Op. cit.*, *sub* 48.

E proprio con il recente d.lgs. n. 61 del 2011[51] si stabiliscono le procedure per l'individuazione e la designazione delle Infrastrutture Critiche Europee (ICE) nei settori dell'energia e dei trasporti, nonché le modalità per la valutazione della sicurezza e le prescrizioni minime di protezione delle Infrastrutture Critiche Europee, in conformità a quanto disposto dalla direttiva europea che recepisce[52].

Dalla normativa europea si cerca di elaborare e definire una classificazione unica per tutte le nazioni, individuando come Infrastrutture Critiche:

- infrastrutture per la produzione, trasporto e distribuzione di energia (elettrica, gas ecc.);
- circuiti bancari e finanziari;
- sistema sanitario;
- infrastrutture di trasporto (aereo, viario, ferroviario, navale ecc.);
- infrastrutture per la raccolta, distribuzione e trattamento delle acque superficiali;
- servizi di emergenza;
- filiera alimentare.

Attualmente le infrastrutture vengono controllate e azionate sempre più spesso da sistemi informatizzati, diversamente da ciò che avveniva fino a poche anni fa dove ciascun sistema era autonomo, senza possibilità di accesso dall'esterno e gestito da operatori interni.

Le esigenze di oggi prevedono invece sistemi di controllo, di automazione, di allarmistica, di geo localizzazione, necessariamente dislocati a struttura orizzontale e ciò li rende inevitabilmente sufficientemente vulnerabili ad attacchi informatici.

Tutte queste infrastrutture vengono gestite attraverso codici prestabiliti; solo nel 2007 sono stati rilevati oltre 23.500.000 attacchi provenienti dal *web*, nel 2009 il numero è salito a oltre 73.500.000 mentre nel 2010 il fenomeno è aumentato a oltre 580.000.000 di invasioni, con la potenziale presenza nelle reti di comunicazione globale di *server web* infetti, sistemi zombie e *botnets*

[51] Con il d.lgs. n. 61 dell'11 aprile 2011 l'Italia ha recepito la direttiva 2008/114/CE dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione. Il decreto legislativo è entrato in vigore il 5 maggio 2011, in G.U. n. 102 del 4 maggio 2011.

[52] Direttiva 2008/114/CE del Consiglio dell'8 dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione in http://www.vigilfuoco.it/allegati/biblioteca/Direttiva.pdf.

che sono solo l'elemento evidente di problematiche di sicurezza molto più complesse[53].

Le operazioni che questi codici effettuano nel loro funzionamento, sono molto simili a quelle di un sistema d'arma: definizione del target, inquadramento del bersaglio, ingaggio dell'obiettivo, calcolo delle variabili, fuoco sul bersaglio, raggiungimento del target, perforazione delle difese esterne, penetrazione dell'elemento distruttivo, abbattimento del bersaglio[54]. Ampie riflessioni le lascia il costrutto teorico su cui di basa la *Net Centric Warfare*: "con la digitalizzazione, si mira ad ottenere il predominio sull'avversario essenzialmente grazie alla superiorità nelle informazioni ed alla condivisione del flusso informativo tra tutti i nodi. In altri termini ciò che prima era funzione di potenza di fuoco e protezione, con la *Net Centric Warfare* diventa funzione dell'*information dominance* e della rapidità, anzi dell'istantaneità, del processo decisionale, dove tale istantaneità può indurre la paralisi nel processo decisionale del nemico impedendogli di fatto di produrre una reazione coerente ed efficace."[55].

Secondo il *Center for Strategic and International Studies* (CSIS) nel ristretto arco temporale di 3 anni (2006-2009), sono stati ben 44 i più significativi *cyber incidents*, il 30% dei quali avvenuti nel solo anno 2009[56], che hanno colpito con successo enti pubblici statali, della Difesa e società tecnologiche, ovvero crimini di natura economica con perdite per oltre 1 milione di dollari.

Si segnalano gli attacchi più significativi reperiti nel rapporto "Le esigenze americane in materia di *cyber* terrorismo e *cyber war*"[57]:

- nel gennaio 2009 ignoti criminali informatici, presumibilmente un'organizzazione della *ex* Unione Sovietica finanziata da Hamas o Hezbollah, hanno attaccato l'infrastruttura Internet di Israele nel corso dell'offensiva

[53] Osservatorio IIASCEPP Settore Sicurezza e Difesa http://formazione.iiascepp.org/public/Osservatorio/GennaioFebbraio_1_2011/Gennaio-Febbraio_2011.pdf.

[54] *Op. cit.*, *sub* 52.

[55] http://www.difesa.it/SMD/CASD/Istituti_militari/CeMISS/Pubblicazioni/Documents/83169_NetCenWarpdf.pdf.

[56] Center For Strategic And International Studies (CSIS), "*Significant Cyber Incidents Since 2006*", november 2009.

[57] S. MELE, *Le esigenze americane in materia di cyber-terrorismo e cyber-warfare. Analisi strategica delle contromisure* http://www.stefanomele.it/publications/default.asp?filtrocerca=&filtrocat=&curpage=2&ord=data&come=desc.

militare nella Striscia di Gaza, paralizzando attraverso 500.000 computer, i siti della pubblica amministrazione;

- nel febbraio 2009 ignoti criminali informatici hanno attaccato e violato i sistemi della *Federal Aviation Administration* (FAA);

- nel luglio 2009 numerosi attacchi informatici di tipo *Distribuited Denial of Service* sono stati perpetrati alle infrastrutture ed ai siti governativi degli Stati Uniti d'America e della Corea del Sud, presumibilmente, dalla Corea del Nord;

- nell'agosto 2009 Albert Gonzalez è stato incriminato per aver rubato tra il 2006 ed il 2008, insieme ad alcuni ignoti complici russi o ucraini, circa 130 milioni di carte di credito e di debito attraverso sistematiche violazioni dei sistemi informatici di 5 grandi imprese americane, commettendo la più importante violazione di sistemi informatici ed il più grande furto di identità della storia degli Stati Uniti d'America;

- nel dicembre 2009 il quotidiano The Wall Street Journal ha riportato la notizia che i sistemi informatici di una tra le maggiori banche americane sono stati violati da ignoti *hacker*, causando una perdita economica di circa 10 milioni di dollari;

- nel gennaio 2010 il colosso dei motori di ricerca Google ha denunciato una profonda violazione nella sicurezza dei propri sistemi informatici e di quelli di una trentina di altre rilevanti Società americane. Google ha attribuito la responsabilità degli attacchi alla Cina;

- nel gennaio 2010 un gruppo noto con il nome di "Iranian Cyber Army" ha violato i sistemi informatici ed interrotto i servizi del noto motore di ricerca cinese Baidu. Gli utenti in navigazione sono stati reindirizzati ad un'ulteriore pagina *web* contenente un messaggio a sfondo politico inneggiante all'Iran (messaggio sostanzialmente identico a quello lasciato nel dicembre 2009 sempre dallo stesso gruppo dopo aver violato i sistemi di *Twitter*, noto *social network*).

Gli esempi riportati fanno immediatamente constatare l'importanza della sicurezza interna di ogni paese verso i potenziali attacchi informatici che possono provenire da qualunque parte e per gli scopi più disparati, da quello terroristico a quello di impatto prettamente economico.

Appare quindi evidente che anche in Italia si debba procedere ad investire in risorse di tutela sul *cyber crime*, onde evitare ingenti danni patrimoniali che statisticamente rappresentano, come prima mostrato, la maggior parte degli eventi aggressivi, andando a colpire il settore produttivo privato.

È da rilevare in particolare che lo Stato Maggiore della Difesa, III Reparto – Centro Innovazione Difesa (CID) si è con successo candidato a guidare la sezione relativa agli aspetti legali *cyber* nel quadro del *Multinational Experiment 7 – Access to the Global Commons*, sponsorizzato dallo US JFCOM – J9. Questa iniziativa, che durerà fino a tutto il 2012, rappresenta per il team italiano di ricerca, un importante coinvolgimento permanente di attori provenienti dalle forze armate e di polizia, dal settore privato e dal mondo accademico e della ricerca[58].

5. Profili vittimologici del reato informatico

"La paura segue il crimine, ed è la sua punizione"
Voltaire

La vittimologia è una disciplina relativamente giovane che ha come oggetto lo studio delle caratteristiche della vittima e le sue relazioni con il soggetto agente.

Le vittime della criminalità informatica rientrano tra le vittime collettive della scienza, ovvero quei gruppi di individui uniti da speciali legami, interessi o fattori di circostanze che li rendono bersaglio o oggetto di vittimizzazione[59].

Le vittime della criminalità informatica (*computer related crime*) sono in forte aumento di pari passo con la diffusione e l'impiego dei computer e di Internet.

In seguito allo sviluppo del collegamento in rete crescono i fenomeni di computer crime, estrinsecandosi in episodi di intrusione in banche dati riservate, e attraverso la diffusione della cosiddetta pirateria informatica, arrivano alla illecita duplicazione, diffusione ed uso di programmi sia di pubblica utilità che di dati privati.

Il numero delle vittime del computer crime è oscuro, per la riluttanza a denunciare l'accaduto, ma anche per l'impossibilità di identificare il reo, oppure per il timore di dover sostenere spese legali che potrebbero risultare maggiori del danno economico sofferto.

In sostanza le cause di tale atteggiamento di reticenza sono da ricercare:

[58] Osservatorio di politica internazionale Cyber security Europa e Italia, n. 32, maggio 2011, Approfondimenti, a cura dell'Istituto Affari Internazionali (IAI) http://www.iai.it/pdf/Oss_Polinternazionale/pi_a_0032.pdf.

[59] P. Fedeli, G. Ricci, C. Cortucci, *Lineamenti di Criminologia*, Napoli, ESI, 2006, p. 163 e ss.

"articoli/devivo" — 2012/4/5 — 10:45 — page 56 — #56

1) nella scarsa fiducia nella Polizia, considerata inesperta a contrastare tale tipo di reati;
2) nella tutela dell'immagine aziendale che potrebbe essere compromessa se la manifestata vulnerabilità informatica venisse resa di pubblico dominio;
3) nella mancata consapevolezza dell'essersi verificato un reato a loro danno;
4) nell'influenza dei consulenti informatici aziendali che, per legittimare la loro presenza, cercano di convincere la *leadership* a risolvere la questione internamente.

Il criminale informatico ha elevata preparazione tecnica, cultura superiore, gode della stima dei colleghi, non ha quasi mai precedenti penali e/o disciplinari[60].

Nonostante il reato informatico sia una figura alquanto giovane nel panorama dei reati, si assiste ad una evoluzione rispetto alle prime azioni criminose che erano volte a colpire i consumatori ignari del fenomeno.

Rispetto agli originari furti di identità dove veniva utilizzata l'identità altrui per commettere truffe a nome di persone del tutto ignare (crimini che comunque continuano a sussistere), i nuovi reati prendono di mira i servizi *on-line* del settore bancario, le loro potenti banche dati, il sistema monetario telematico ed il commercio elettronico.

Di seguito si riportano le competenze in *computer related crime* evidenziati dalla Procura della Repubblica di Milano[61]:

- *dialer* (numerazioni a valore aggiunto);
- furto di identità semplice;
- violazione *account*;
- accesso *e-mail*;
- altro accesso abusivo a sistemi informatici;
- truffa *e-Bay* o su altre piattaforme di *e-commerce*;
- bonifico/ricarica disconosciuta (*phishing*);
- riciclaggio elettronico proventi illeciti (*cyberlaundering*).

Da questi reati inevitabilmente ne discendono altri ad essi collegati, infatti è emerso che si è altamente specializzato il riciclaggio delle somme, talvolta cospicue, che questi criminali riescono a sottrarre alle vittime. In realtà l'organizzazione vede un numero ingente di soggetti che dietro provvigione,

[60] *Op. cit.*, *sub* 58.

[61] http://www.procura.milano.giustizia.it/ho-bisogno-di-altre-informazioni-sui-reati-informatici.html.

invia le somme truffate all'estero, spesso all'*ex* blocco sovietico, le ricicla e le re-immette in ricariche di schede telefoniche prepagate utilizzate per chiamare numeri a tariffazione speciale. Questo sistema è utilizzato soprattutto dalla criminalità rumena[62].

I fenomeni devianti più comuni sono:

- il *phishing*[63]
- il *pharming*[64]
- la monetica[65]
- il *bot*[66]

Il *phishing* è una frode informatica che, attraverso il furto di identità, induce gli utenti a rivelare informazioni e codici riservati e con essi si compiono illeciti come prelievi bancari e ricariche telefoniche. Spesso questi dati vengono rivenduti al mercato nero dell'illecito ricavando profitto, utilizzando i codici carpiti con l'inganno e truffando gli ignari possessori del numero.

Negli ultimi anni i *phisher* sono diventati sempre più esperti, iniziando ad utilizzare *crimeware* che, colpendo le vulnerabilità dei *browser web*, infettano i computer delle vittime. Infatti sarà il *Trojan Horse* o lo *spyware* installato sul computer ad intercettare queste informazioni non appena l'utente visiterà il sito *web* legittimo della propria banca o di altro servizio *on-line*, oltretutto i sistemi sono così mirati che intercettano solo le informazioni necessarie al *phisher* e l'utente non si accorge affatto di avere un computer infettato.

Il *pharming* è un'azione simile al *phishing*, tuttavia, anziché sollecitare direttamente informazioni personali o aziendali, dirotta URL legittimi e li reindirizza, attraverso il *server* dei nomi di dominio, a indirizzi IP fraudolenti che falsificano gli originali. Questi URL sottoposti a *spoofing* raccolgono, utilizzando un'interfaccia utente grafica, informazioni protette senza che nessuno si accorga della differenza. Dal momento che il *pharming* richiede capacità tecniche superiori (e poiché il *server* DNS è molto difficile da manipolare), questa tecnica è molto meno comune del *phishing*, ciò nonostante è

[62] A. APRUZZESE, *Autori e vittime nella criminalità informatica*, in "Rivista di Criminologia, Vittimologia e Sicurezza", Vol. 3-4, 2009-2010, nn. 3-1.

[63] http://www.crime-research.org/news/09.11.2005/1614/ http://www.csoonline.com/article/221737/phishing-thebasics, Convegno "La sicurezza dei cittadini nelle aree metropolitane" (Roma, 25 ottobre 2010).

[64] http://teca.elis.org/2716/prevenzione-repressione-crimini-informatici-2009-12-02.pdf.

[65] A. MUSCELLA, *L'altra faccia della Monetica*, Registrazione SIAE n. 2010001267.

[66] *Op. cit.*, *sub* 61.

ancora possibile che il *pharming* diventi una minaccia crescente nel prossimo futuro.

La "monetica" è un nuovo settore che contempla le truffe monetarie con l'informatica, ed è particolarmente colpita dai traffici illeciti di identità a livello aziendale. Oltre ai sempre più diffusi e gravi episodi di clonazione di carte di credito e di altri sistemi elettronici di pagamento, furti di milioni di riservati codici di carte di credito vengono oggi realizzati mediante attacchi informatici alle sempre più diffuse banche dati che elaborano e gestiscono l'enorme flusso del commercio elettronico[67]. Esiste un mercato mondiale di codici di conti bancari *on-line* gestito da bande criminali che sfruttano e rivendono ad altri le informazioni ed i codici stessi.

Il *bot* è l'abbreviazione di robot, ed è uno dei crimini informatici più sofisticati, tra tutti quelli che mettono a rischio gli utenti di Internet, sono simili ai *worm* e ai *Trojan Horse*, ma ricevono questo appellativo in quanto svolgono un'ampia varietà di attività automatiche per conto di un mandante (i criminali informatici). Le attività che possono essere svolte dai *bot* variano dall'invio di *spamming* alla paralisi di siti *web* nel quadro di un attacco di tipo "*denial-of-service*" coordinato. Poiché un computer infettato da un *bot* obbedisce agli ordini del proprio controllore, molte persone si riferiscono a questi sistemi vittima chiamandoli "zombie". I *bot* sono così invisibili che talvolta le vittime ne vengono a conoscenza solo quando il fornitore di servizi Internet le informa che il loro computer sta inviando messaggi di *spamming* ad altri utenti di Internet.

Abbiamo analizzato le più comuni forme di infezioni e manipolazioni del pc per affrontare il discorso sulla vittima di questi reati.

Diversamente dai reati comuni, non si riesce a fornire in dottrina una categoria di vittime che possa risultare più esposta a questo fenomeno, forse l'unica classificazione fattibile è quella di "vittima collettiva", ovvero gruppi o raggruppamenti di individui uniti da speciali legami, interessi o fattori di circostanze che li rendono bersaglio o oggetto di vittimizzazione.

Parlare di vittime collettive significa, molto spesso, considerare individui che sono oggetto di reati che non colpiscono una persona determinata, ma che offendono un interesse appartenente ad una collettività indeterminata di persone. Queste, sovente, neppure percepiscono il reato come lesione dei loro interessi, come ad esempio accade nei reati di frode alimentare,

[67] *Op. cit.*, *sub* 61.

nei reati ambientali, nei reati commessi dalla stessa autorità in relazione alla commistione tra potere politico e affaristico.

Ogni soggetto che usi la tecnologia informatica può diventare vittima, essendo del tutto ininfluente l'età, la cultura, la professione o le abitudini sessuali, criteri questi che influiscono grandemente nella potenziale vittima dei reati comuni.

Ad esempio nel *cyber stalking*, ovvero le molestie via Internet (invio di *spam*, messaggi non graditi, insulti *on-line*, ecc.) l'autore di queste molestie nemmeno identifica la sua vittima, che potrebbe essere sia uomo che donna, di ogni età e professione, dal momento che, come è noto, il reato informatico è un reato senza vittima (identificata!!).

Per questo tipo di illeciti sarebbe opportuno sensibilizzare la collettività in ordine alla loro tutela ed approntare un più esteso riconoscimento degli enti esponenziali ed un maggiore inasprimento delle sanzioni considerando l'effetto deterrente che producono.

Attualmente le maggiori associazioni dei consumatori ricevono numerose segnalazioni di danno dal parte degli utenti di Internet, talché già da diverso tempo hanno approntato dei formulari prestampati per la raccolta della segnalazione e per la conseguente azione legale.

Si riportano di seguito delle testimonianze di vittime di reato informatico.

Articolo dell'Ansa-Reuters[68]: anche la Epson vittima degli *hacker*: dalla divisione in Sud Corea dell'azienda giapponese sono stati rubati i dati di 350 mila clienti. Un portavoce dell'azienda ha spiegato che oltre ai nominativi e alle *mail*, sono stati sottratti numeri di telefono e dati sugli acquisti. Il caso è stato sottoposto alla *Communications Commission* che da tempo si occupa di sicurezza informatica in un Paese in cui si sono registrate tante intrusioni in siti privati e governativi. "Stiamo ancora indagando sul caso e cercando di individuare gli *hackers*", ha detto un portavoce della commissione. La Corea del Sud sta lavorando su un grande piano di sicurezza dopo l'ondata di attacchi contro agenzie governative, aziende e compagnie finanziarie esposte alla vulnerabilità di Internet, in uno dei paesi più in rete del mondo. A fine luglio sia il portale Nate Internet che il sito *Cyworld blogging*, entrambi di proprietà di Sk Comms, sono stati violati e gli *hacker* hanno attinto alle informazioni di 35 milioni di utenti, l'attacco più grosso di tutti i tempi nel paese, attribuito alla Cina. E in aprile la Nonghyup, una grande banca

[68] http://www.primaonline.it/2011/08/22/95380/epson-hacker-rubano-dati-di-350-mila-clienti/.

commerciale a partecipazione statale, ha avuto un crollo della rete interna che ha causato problemi a milioni di clienti. Questa volta la paternità della violazione è stata attribuita alla Corea del Nord che ha respinto le accuse.

Ulteriore testimonianza del reato informatico[69]: "La peggiore beffa che avrei mai potuto immaginare". Così commenta V.B., ventinovenne spoletina, ripercorrendo le tappe della frode informatica di cui è stata vittima nel giugno scorso. Nei mesi precedenti la malcapitata aveva messo da parte 700 euro nel suo conto BancoPosta *on-line* per pagare un corso di perfezionamento professionale. È stato solo pochi giorni prima di effettuare il versamento della tassa d'iscrizione che V.B., controllando il saldo da uno sportello bancomat, ha fatto l'amara sorpresa. La cifra che, incredula, si è trovata di fronte era di poco più di 8,71€. Nella lista dei movimenti risultavano essere stati effettuati due prelievi, a distanza di una settimana l'uno dall'altro, rispettivamente di 500 e 160€. I movimenti erano contrassegnati come "addebito per ricarica su carta prepagata da BPOL". In sostanza qualcuno aveva effettuato quei prelievi dal suo conto verso un'irrintracciabile carta di credito. Presa dal panico per l'impellente necessità di quel denaro, la giovane si è recata immediatamente all'ufficio postale in cui aveva aperto il suo conto per chiedere spiegazioni. "L'unica cosa che possiamo fare è chiamare il numero verde di Poste Italiane, ma la mia situazione non sembrava colpire più di tanto gli impiegati", racconta la malcapitata. Seguendo scrupolosamente le istruzioni ricevute, la ragazza si è poi recata presso il Commissariato di Polizia di Spoleto per denunciare l'accaduto. La ragazza ha provveduto successivamente a telefonare alla Polizia Postale per avere chiarimenti in merito, nella speranza che qualcuno potesse svelarle la dinamica di una simile frode. "Non ho mai comunicato, né verbalmente né per iscritto, i miei codici ad alcuno – ricorda la studentessa – men che mai ho risposto ad alcuna *mail* potenzialmente di *spam* o *phishing*". "Con mio grande stupore nessuno è sembrato particolarmente colpito dall'accaduto, né ha saputo o voluto rincuorarmi circa la possibilità di un eventuale rimborso". È stato a questo punto che la giovane spoletina ha deciso di rivolgersi ad un avvocato, per tentare di recuperare il denaro indebitamente sottrattole dall'ignoto malvivente. Da parte di Poste Italiane, infatti, la possibilità di rivedere i suoi soldi veniva paventata come una pallida quanto remota possibilità. "È una cosa che ancora non mando giù", continua V., "possibile che non esista un modo per tutelare i correntisti che, confidando nella sicurezza del sistema, affidano i propri risparmi in

[69] Articolo del 26 marzo 2010, http://tuttoggi.info/articolo/21668/.

un conto *on-line*?". Per nove mesi Poste Italiane non ha fornito spiegazioni esaurienti. Di appena una settimana fa, una lettera delle Poste ha informato la sventurata che l'indagine della Polizia Giudiziaria è tuttora in corso e che la sua posizione potrà essere valutata a conclusione delle stesse.

Altro esempio di frode *on-line* da una lettera all'associazione dei consumatori ADUC[70]: "Cara ADUC, premetto di essere abbonato con una compagnia telematica la quale mi fornisce la linea ADSL pagando un canone fisso bimestrale di 85 euro. Nella data di ieri mi giungeva la fattura sulla quale la compagnia mi addebitava un importo di 758 euro di canone telefonico e 573 euro di chiamate vocali in Somalia che non ho mai fatto. Preciso che le chiamate sono state fatte attivando una linea voip che si attiva semplicemente *loggandosi* nell'area utente della compagnia senza dover firmare nessun modulo. La compagnia dice che si tratta di una frode che hanno compiuto ai miei sistemi quindi la compagnia non può essere responsabile di tale situazione. Per il recupero dei soldi mi hanno detto che è necessario effettuare una denuncia alla Polizia Postale in modo da rintracciare il malfattore. In data odierna, contattavo tramite il servizio *e-mail* un operatore della compagnia riferendo che le chiamate a me addebitate non sono state effettuate dal sottoscritto e quindi mi sembra giusto che non le paghi. L'operatore con altra *e-mail* mi riferiva che possono stornare la cifra del canone di 758€in modo da venirmi incontro mentre il costo delle chiamate di 573€mi tocca pagarlo perché sono dei costi che anche la compagnia sostiene. Conclusione, la compagnia si ritiene non responsabile di questo accaduto: il malfattore è entrato nei miei sistemi e una volta rubato la password ha effettuato attivazioni di linee telefoniche ed ha effettuato le telefonate. Poco tempo fa ho fatto denuncia ai Carabinieri i quali poi passeranno la pratica alla Polizia Postale".

6. Computer forensic e tracciabilità

"La legge non può in nessun caso violare
i limiti imposti dal rispetto della persona umana"
Costituzione della Repubblica Italiana, Art. 32

I temi ricorrenti che vengono analizzati quando entrano in gioco le tecnologie nella soluzione di un crimine, sono sostanzialmente tre: la tracciabilità, la prova e la *privacy*.

[70] Lettera all'ADUC, 13 dicembre 2010, http://sosonline.aduc.it/scheda/diffida_9605.php.

Nel nuovo contesto criminologico informatico l'attenzione viene subito focalizzata sulla tracciabilità dei soggetti, vittima e/o indagato, coinvolti nella scena del crimine.

Le attività investigative, sia tradizionali sia digitali, partono immediatamente dalla possibilità di controllare se uno o più soggetti al momento dell'evento si trovavano "nei pressi della", "nella" o "lontano dalla" scena del crimine. E così, in una attività investigativa di tipo digitale, si cercano i cellulari, le schede; si tracciano le celle; si raccolgono gli sms; si monitorizzano le chiamate e gli orari collegati agli scambi telefonici; si cerca nelle identità virtuali dei soggetti coinvolti; si controllano la pagine su *facebook*, le *e-mail*, le amicizie virtuali, il tempo passato al pc, cercando di tracciare gli spostamenti virtuali e no di colui che afferma essere stato in un determinato luogo invece che in un altro.

L'oggetto di questa ricerca è un individuo che incarna le peculiarità della società basata sull'ICT, un soggetto che considera, cioè, la rete come parte inscindibile della propria esistenza. È con questa nuova tipologia di "uomo 2.0" che il diritto si confronta, ormai, costantemente.

L'uomo 2.0 è colui che esiste solo se appare e solo se appare in rete, ancor meglio se è presente nei *social network*. Le informazioni che riguardano questo individuo subiscono la sua stessa trasformazione, diventando dati informatici contenuti in *file* e trasmessi attraverso la rete o semplicemente gestiti dalle USB, *memory card*, cellulari, *smart card* e piattaforme digitali su cui si sviluppano i *social network* e le realtà virtuali.

Da questo ambiente, una volta entrati, è impossibile sfuggire ma soprattutto è impossibile agire senza lasciare traccia.

7. (CONTINUA) PRIVACY, ANONIMATO, ANONIMATO E IDENTIFICAZIONE: IL PROBLEMA DELL'IP, ANONIMATO E QUADRO NORMATIVO, DIRITTO ALL'OBLIO

"Una rete a maglie fittissime viene stesa su tutta la società,
che consente di seguire implacabilmente
ogni traccia lasciata da ciascuno di noi, ricostruendo l'insieme
dei rapporti sociali attraverso l'individuazione
di tutte le persone chiamate, il luogo e la durata delle telefonate.
Il rischio di abusi è evidente"
Stefano Rodotà, "Se nasce l'uomo a barre, La Repubblica, 1999"

Quando si parla di tracciabilità si pensa immediatamente alla *privacy* ed

al suo rapporto con la sicurezza pubblica.

Una particolare attenzione è riservata alla tutela dei diritti fondamentali ed alla lotta alla criminalità informatica, laddove gli strumenti informatici entrano a far parte della *scena criminis*.

A causa del fenomeno del terrorismo gran parte dei Paesi Europei si sono mossi aumentando i controlli sulle comunicazioni non solo telefoniche ma soprattutto telematiche, nell'intento di proteggere i propri cittadini e la sicurezza dei propri territori. Il fenomeno è conosciuto come *data retention*.

La prima cosa a cui si è provveduto, non senza forti contrasti, è stata l'istituzione dell'obbligo di conservazione dei dati di traffico telefonico e telematico da parte dei "soggetti coinvolti nella gestione" del traffico stesso. Per dati di traffico si intendono i dati identificativi del chiamante: la data, l'ora, la durata della chiamata; l'identificativo del destinatario e così via. Tutto ciò per permettere all'autorità inquirente di analizzarli, in caso di necessità.

Le perplessità sorgono nel potenziale pericolo di un indiscriminato monitoraggio degli utenti, ma è stato più volte evidenziato che oggetto dell'analisi da parte dell'autorità competente non sono i contenuti delle comunicazioni bensì i dati inerenti il traffico delle stesse.

Autorevole dottrina avverte che "sapere con chi un soggetto è in comunicazione – anche senza conoscere il contenuto della stessa – costituisce una forma di sorveglianza informatica ancor più invasiva del c.d. braccialetto elettronico utilizzato per controllare gli spostamenti dei detenuti in regime di semi-libertà. Si potrebbe dunque ritenere che il principio della libertà e della segretezza delle comunicazioni debba dunque estendersi al mero dato di traffico perché esso, di per sé, è rilevatore della sfera privata del soggetto che va protetta"[71]. Distinguere il dato dal suo contenuto, a volte, diventa impossibile, soprattutto laddove è il dato stesso a "parlare" e a rivelare tutto di un soggetto, così come l'uso della carta di credito o del cellulare che permette di tracciare i movimenti dell'individuo.

L'art. 132 del d.lgs. n. 196 del 2003 prevede nel co. 4 *ter* la conservazione dei dati di traffico fino ad un massimo di sei mesi, per fini di indagine, fermo restando quanto disposto dal successivo co. 4 *quinquies*.

È bene ricordare, tuttavia, che la lotta al terrorismo non può sacrificare i princìpi cardine della democrazia. Nel lontano 1755, Beniamin Franklin

[71] V. ZENO ZENCOVICH, *Repressione della criminalità informatica e tutela dei diritti fondamentali*, in "D & Innovazione", 2008, n. 7, consultabile anche *on-line* all'indirizzo: http://www.dirittoestoria.it/7/D-&-Innovazione/Zeno-Zencovich-Criminalit-informatica-tutela-diritti.htm.

rispondendo al Governatore della Pennsylvania dichiarò che colui che "(...) è pronto a dar via le proprie libertà fondamentali per comprarsi briciole di temporanea sicurezza non merita né la libertà né la sicurezza". La Corte di Giustizia europea ha ribadito con forza il principio nelle decisioni inerenti i casi Khadi, Al Barakhaat Foundation e Omar Mohammed Othman[72]. In esse è ribadita la contrarietà a qualsiasi deroga che comprometta i princìpi di libertà e di democrazia o comunque di tutela dei diritti dell'uomo (specificamente i diritti della difesa ed il diritto al contraddittorio) ai quali l'intera Unione Europea da sempre si ispira.

Nell'ambito delle investigazioni digitali, l'aspetto legato alla *privacy* dell'individuo ed i correlati diritti all'anonimato ed all'oblio, rappresentano un ulteriore motivo di riflessione[73].

Il diritto ha da sempre avvertito la forte esigenza di garantire l'individuo, con i suoi diritti e le sue libertà, da eventuali pericoli della rete. Il d.lgs. n. 196 del 2003, meglio noto come "Codice della privacy", è stato "il" prodotto più approfondito e completo redatto dal nostro legislatore, ispirandosi ad un tipo "di approccio 'tecnologicamente neutro', ossia valido ed applicabile a tutte le forme di comunicazione elettronica a prescindere dal mezzo utilizzato"[74].

[72] Sui casi *Khadi* e *Al Barakhaat*, cause riunite in tema di terrorismo internazionale, si sono pronunciati: il Tribunale di primo grado (21 settembre 2005) e, successivamente, la Corte di giustizia, con la sentenza del 3 settembre 2008; sul caso Othman il Tribunale di primo grado con sentenza 11 giugno 2009. Il testo integrale delle decisioni sono reperibili in http://curia.europa.eu/juris/document/document.jsf?docid=75450&doclang=it&mode=&part=1. Sul caso Othman v. anche una interessante nota di P. PIRRONE, *Ancora sui rapporti tra ONU e CE in materia di lotta al terrorismo e tutela dei diritti fondamentali: la sentenza del Tribunale di primo grado nel caso Othman*, in "Diritti umani e diritto internazionale", Vol. 3, 2009, n. 3, p. 654. http://curia.europa.eu/juris/index_form.htm

[73] Dottrina e giurisprudenza hanno prodotto materiale di studio abbondante sulla *privacy*. Cfr. per tutti: S. SICA, P. STANZIONE (a cura di), *La nuova disciplina della privacy d.lgs. 30 giugno 2003, n. 196*, Bologna, Zanichelli, 2005, *passim*; A. ZUCCHETTI, *Privacy. Dati personali e sensibili. Sicurezza, regolamento, sanzioni. Problemi e casi pratici*, Milano, Giuffrè, 2005, passim; T.M. UBERTAZZI, *Il diritto alla privacy. Natura e funzione giuridiche*, Padova, Cedam, 2004, *passim*; S. RODOTÀ, *Intervista su privacy e libertà*, Bari, Laterza, 2005, *passim*; F. CARDARELLI, S. SICA, V. ZENO ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Milano, Giuffrè, 2004, *passim*; C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196*, Padova, Cedam, 2007, *passim*; G. PASCUZZI, *Il diritto dell'era digitale*, Bologna, Il Mulino, 2010, *passim*.

[74] A. MAGGIPINTO, M. IASELLI, *Sicurezza e anonimato in rete. Profili giuridici e tecnologici della navigazione anonima*, Milano, Nyberg, 2005, p. 16.

È bene ricordare sinteticamente cosa si intende per *privacy* e cosa per anonimato.

Quando "si è" in rete, lavorare, giocare e persino oziare, diventa visibile. I dati che riguardano le attività oppure semplicemente l'identità di un individuo sono ovunque e sono accessibili in ogni momento e da qualunque luogo ci si colleghi. Parlare di *privacy* in questo contesto sembra una contraddizione in termini. Ma bisogna ricordare che il concetto di *privacy* non si esaurisce nel diritto ad "essere lasciato in pace", ossia di escludere soggetti non autorizzati ad entrare nella propria sfera personale, bensì si esplica nel diritto (ulteriore) ad avere il controllo sui propri dati.

Nel nostro ordinamento, questo diritto è ormai pacificamente collocato tra i diritti fondamentali della persona[75] così come lo è a livello europeo[76]. Per quanto riguarda i riferimenti normativi in materia, oltre al già citato d.lgs. n. 196 del 2003, il legislatore europeo ha prodotto la famosa direttiva 95/46/CE che tratta della c.d. "computer privacy", ossia della sicurezza informatica ed all'interno della quale si fa una ulteriore precisazione laddove sono previsti dei veri e propri limiti alla tutela della *privacy* dei cittadini in tutti quei casi in cui sia in giuoco la sicurezza nazionale e quella pubblica (art. 13)[77]. A seguire: la direttiva 2002/58/CE sul Trattamento dati personali e la tutela della vita privata nel settore delle comunicazione elettroniche e la più recente direttiva del 2009/136/CE. Tutti gli interventi del legislatore europeo hanno rivelato l'intento di assicurare all'individuo (l'interessato) un controllo (che sarebbe più opportuno definire un vero e proprio "diritto di seguito") sui propri dati[78].

Le indagini digitali, legate alla *privacy*, possono riguardare il controllo di *file* e di cartelle su di un pc aziendale, per verificare l'esistenza di materiale

[75] Diritti inviolabili dell'uomo *ex* artt. 2, 14, 15 e 21 della nostra Costituzione. In dottrina: V. ZENO ZENCOVICH, *Personalità (diritti della)*, in "Digesto civile", XIII, Utet, 1995, p. 430 e ss. e bibliografia *ivi* citata.

[76] Cfr. la Carta dei diritti fondamentali UE, art. 8, la Convenzione europea dei diritti dell'uomo, art. 8 e l'art. 16 del Trattato sul funzionamento dell'Unione Europea.

[77] Richiamati anche gli artt. 6, 10 ed 11. Le ipotesi di limitazione alla tutela della *privacy* hanno trovato applicazione, a livello nazionale, con l'emanazione della l. 31 luglio 2005, n. 144 per la lotta al terrorismo.

[78] Sulla "dinamicità" della natura di questo diritto così come sulla sua particolare complessità che si articola in una serie di sfaccettature quali: il diritto di conoscenza, di accesso ai dati, di aggiornamento degli stessi, il diritto all'oblio e il diritto di opposizione cfr. G. PASCUZZI, *Il diritto dell'era digitale*, cit., p. 52 e p. 57.

pornografico[79]; oppure possono avere ad oggetto l'analisi delle identità elettroniche, al fine di prevenire o arginare i furti di identità; o, ancora, possono indirizzarsi verso l'esame dei profili pubblicati sui *social network*, al fine di tracciare la personalità della vittima o dell'indagato.

In riferimento allo specifico aspetto dell'anonimato, il diritto privato ne tratta sotto vari aspetti, ad esempio nei rapporti familiari (diritto all'anonimato di una madre o di un padre); nelle ipotesi del diritto di un donatore a restare anonimo; nel diritto d'autore laddove questi decida di restare anonimo ed, ovviamente, nel caso della protezione dei dati personali. Ma si parla di anonimato anche nel diritto penale, ad esempio nei reati che riguardano minacce, notizie anonime di reato, diritto all'anonimato da parte dei collaboratori di giustizia o dei testimoni c.dd. a rischio, ecc.; nel diritto amministrativo, in riferimento ai concorsi pubblici o agli appalti; e, infine, nel diritto costituzionale (diritto di libera manifestazione del pensiero)[80].

In questo contesto interessa analizzare l'anonimato con riferimento alla rete ed ai dati personali.

La definizione di anonimato più articolata e completa è contenuta nel testo del "Codice della privacy" che all'art. 4, co. 1, lett. *n*), definisce il dato anonimo come: "(...) il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile". Nel "Codice della privacy" si parla, dunque, di anonimato inteso come "dato" riferito ad una determinata persona. Infatti, il legislatore europeo lo etichetta come "informazione personale"[81]. In realtà nel Codice quando si parla di dato anonimo non si intende parlare dell'anonimato inteso come diritto. Il dato anonimo, per il Codice, è quello contrapposto al dato personale, ossia un dato comune o generico.

Quando si parla di anonimato in rete appare subito evidente una sorta di profonda frattura tra chi sostiene il diritto di agire in anonimato (che equi-

[79] Cfr. in tal senso uno degli ultimi provvedimenti emanati dal Garante della privacy del 10 giugno 2010, doc. *web* n. 1736780, in Bollettino del n. 118/giugno 2010, http://www.garanteprivacy.it/garante/doc.jsp?ID=1736780.

[80] Cfr. per tutti E. PELINO, *L'anonimato su Internet*, in Finocchiaro G. (a cura di), "Diritto all'anonimato. Anonimato, nome e identità personale", Padova, Cedam, 2008, p. 289 e ss.; per l'aspetto specifico inerente il "diritto all'anonimato" e il "diritto penale", *ivi*, p. 176 e ss. e A. MAGGIPINTO, M. IASELLI, *Sicurezza e anonimato in rete*, cit., p. 9 e ss.

[81] Per la prima volta nella risoluzione europea del Consiglio d'Europa n. 22 del 1973. Concetto più volte ripreso in seguito da altre Risoluzioni fino ad essere ribadito nella Convenzione di Strasburgo per la protezione delle persone in relazione al trattamento dati, del 28 gennaio 1981 (art. 2, co. 1).

vale, sostanzialmente, a non presentarsi con la propria identità) e chi ritiene che l'anonimato non può essere riconosciuto come un diritto in quanto permetterebbe il verificarsi di atteggiamenti illeciti, senza la possibilità di rintracciarne l'autore (come ad esempio nel caso di diffamazione in rete).

Il problema sorge in quanto l'ambiente Internet consente una diffusione virale delle informazioni che sono, di fatto, in grado di rimbalzare senza controllo di *blog* in *blog* o sui vari *social network*. In un simile contesto una notizia falsa o diffamatoria è in grado di procurare gravi danni.

Appare subito evidente quanto sia difficile, per chiunque, prendere una posizione equa sul fenomeno.

L'anonimato se è praticato nei Blog, nei Forum o nelle Chat, può rappresentare una espressione del diritto alla libertà di pensiero; ma, nelle ipotesi di transazioni commerciali (ad esempio nel commercio elettronico), può creare problemi in merito alla sicurezza, nascondendo attività illecite e dunque dannose.

Si riallaccia all'anonimato la c.d. *Privacy Enhancing Technology* (alias PET), che la Commissione europea[82] ha sostenuto con interventi mirati. La PET è sostanzialmente un insieme di tecnologie predisposte per tutelare la *privacy* in settori dove i dati personali transitano normalmente (informazione e comunicazione[83]). L'*anonymizer* potrebbe rappresentare un esempio di tecnologia PET[84].

A favore dell'anonimato si contano tutti quei casi in cui è stata possibile una forma di comunicazione e di informazione libera, senza censura e globale. Si pensi a tutti quei casi in cui il ruolo svolto dalla rete è stato determinante per portare a conoscenza movimenti di protesta di massa come quelli di Teheran, "dove garantire l'anonimato di chi informava il mondo tramite *Twitter* di quanto accadeva per le strade della capitale iraniana era una que-

[82] Il testo del documento che tratta degli interventi europei in materia di PET è consultabile nel sito del Garante italiano http://www.garanteprivacy.it/garante/document?ID=1531367.

[83] L'importanza delle informazioni nella nostra società è stigmatizzata perfettamente nella frase "an age of information about readers as an age of information for readers" di J. E. COHEN, *A right to read anonymously: a closer look at "Copyright Management" in Cyberspace*, in "Connecticut Law Review", Vol. 28, 1995-1996, p. 981, consultabile anche *on-line* all'indirizzo: http://heinonline.org/HOL/Page?men_tab=srchresults&handle=hein.journals/conlr28&id=991&size=2&collection=journals&terms=readers&termtype=phrase&set_as_cursor=, sono richiesti *username* e *password*.

[84] Sull'argomento, per approfondimenti e relativa bibliografia si rinvia a G. PASCUZZI, *Il diritto dell'era digitale*, cit., p. 80 e note.

stione di vita o di morte" e di quanto, in questo caso, sia stato determinante e provvidenziale il fattore dell'anonimato.

Contro l'anonimato si ricordano tutti gli episodi in cui si è abusato della credibilità della "notizia" e della facilità di diffusione della stessa pubblicando informazioni del tutte false[85].

Alcuni casi hanno, poi, una connotazione del tutto particolare: si pensi a fenomeni come Wilkileaks ed il meno conosciuto *Cryptome*[86], quest'ultimo è un sito nel quale è possibile reperire materiale sui metodi di indagine utilizzati dagli investigatori per ottenere informazioni e rintracciare prove[87].

Prospettare una soluzione all'annoso problema è difficile; tra i tanti suggerimenti si potrebbe pensare all'utilizzo di appositi filtri, da parte dei responsabili dei servizi di diffusione delle informazioni *on-line*, compresi i *social network*. Ma una ipotesi di questo tipo non è semplice da attuare, sia a causa della enorme mole di lavoro che si prospetterebbe sia per la sostanziale soggettività delle scelte che verrebbero operate nella delicata fase della decisione di cosa potrà essere considerato lecito o illecito e quindi "pubblicabile" oppure no. Le conseguenze potrebbero essere peggiori del male che si tenta di arginare. I pericoli principali potrebbero consistere in una latente forma di censura oppure nell'alterazione della tipica caratteristica della comunicazione di rete, ossia la sua democraticità[88].

È bene ricordare che in rete è possibile lavorare come utente attraverso un indirizzo IP e pertanto inviare un messaggio reso in forma anonima, ossia non "firmato" (nel senso: "privo dell'indicazione del nome e del cognome dell'autore"), tuttavia ciò non implicherebbe l'impossibilità di identificazione del soggetto che l'ha inviato. "Infatti, tecnicamente, è possibile risalire all'indirizzo IP del soggetto che ha inviato il messaggio eventualmente diffa-

[85] Tra i numerosissimi casi è emblematico quello dei c.dd. "voli gratuiti offerti dalle compagnie aeree americane per personale medico che fosse pronto a partire per Haiti" durante la tragedia che colpì il territorio. Notizia che poi si rivelò una vera e propria "bufala".

[86] L'indirizzo è cryptome.org.

[87] In questi casi ci si pone la domanda se sia giusto pubblicare documenti delle varie diplomazie degli Stati di tutto il mondo, scoprendo giochi di potere sconosciuti ai più, nel rispetto, così, di un'informazione libera e trasparente al servizio del cittadino, ma rischiando di violare "segreti" (di Stato o investigativi) a volte necessari per conservare equilibri diplomatici oppure, nel caso di modalità di indagine, utili laddove determinate procedure investigative proprio grazie alla loro "segretezza" risultano efficaci contro il crimine.

[88] La democraticità, in questo contesto, fa riferimento alla sostanziale immediatezza del canale, intesa sia come comunicazione effettuata in tempo reale sia come comunicazione che non viene mediata da alcuno.

matorio e, tramite l'*Internet Service Provider*, risalire all'identità del soggetto a cui l'IP è stato assegnato, sia esso un IP statico o dinamico". Si innesta in questo contesto, un ulteriore approfondimento, tipicamente giuridico, ossia la natura dell'IP, se cioè possa considerarsi dato personale qualora il titolare del trattamento possa collegarlo a qualche altro dato che consenta una identificazione univoca del soggetto a cui fa riferimento[89].

È evidente che, nella maggior parte dei casi, l'indirizzo IP non è in grado di consentire la immediata identificazione di una persona fisica e, pertanto, non può definirsi un dato identificativo "forte", anche in considerazione del fatto che generalmente gli IP sono dinamici. Ma la norma ribadisce che è dato personale anche una informazione che consente di identificare una persona indirettamente, cioè incrociandola con altri dati, come, ad esempio l'orario di connessione, oppure l'accesso ad una postazione controllata (ad esempio in un *Internet point* o in una biblioteca comunale o universitaria ecc.). Tali dati, utilizzati insieme, consentono di identificare una persona fisica, grazie ai *file* di *log* del fornitore di connessione ad Internet[90]. Pertanto se ne può dedurre che l'IP solo se analizzato isolatamente non è in grado di identificare/profilare un soggetto[91].

Un caso emblematico si è verificato nel 2009. Un Tribunale di Seattle si è espresso in seguito ad una *class action* contro la Microsoft. Nella decisione

[89] L'art. 4, d.lgs. 196/2003 (T.U. dati personali) così recita: "b) 'dato personale', qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

[90] L'indirizzo IP "da solo" non sarebbe, dunque, sufficiente per condannare un soggetto per aver scaricato illecitamente un *file*, ma occorrono altri elementi per poter stabilire che sia "quel" determinato soggetto (e non altri che hanno la possibilità di accedere alla stessa connessione Internet) ad aver commesso "quel" determinato reato.

[91] Secondo il Parlamento Europeo, l'indirizzo IP è da classificarsi tra i dati personali e da trattare come tale, cioè nel rispetto delle leggi sulla *privacy*. In merito si è espresso anche l'Articolo 29 (*Data Protection Working Party* che è un organo consultivo indipendente il quale riunisce le autorità per la protezione dei dati di tutta l'UE) che ha formulato un parere (documento 4/2007) sul concetto di dati personali (WP 136), in http://www.garanteprivacy.it/garante/document?ID=1487717. Anche secondo il Garante l'indirizzo IP rientra tra i dati personali, tant'è che nella policy del sito del Garante (http://www.garanteprivacy.it/garante/doc.jsp?ID=36573) gli IP vengono inclusi tra i dati personali dalla stessa Authority. La giurisprudenza europea recentemente si è espressa a favore dell'IP come dato personale. Così una sentenza emessa l'8 settembre 2010 dal Tribunale federale di Losanna http://www.edoeb.admin.ch/aktuell/01688/index.html?lang=it nella quale si evidenzia che gli indirizzi IP devono essere considerati dati personali e pertanto devono sottostare alla legge sulla protezione dei dati.

si è, di fatto, disconosciuta la potenzialità dell'IP di identificare un individuo. Il giudice ha affermato che, affinché le informazioni possano considerarsi dati personali debbono essere in grado di identificare "davvero" una persona, mentre un IP è in grado di identificare "solo" un computer. All'epoca, contro la decisione, si schierò la EPIC (*Electronic Private Information Center*)[92].

La legge ammette una probabile contrazione del diritto all'anonimato dinanzi ad altri diritti prevalenti. Ma se la formula è chiara, non lo è la sostanza, perché non è affatto facile stabilire quali sono questi diritti prevalenti e quando possono prevalere sul diritto all'anonimato. L'esempio classico è quello della diffamazione *on-line*, dinanzi alla quale il diritto all'anonimato, anche qualora sia connesso con il diritto di libera manifestazione di pensiero o di diritto alla protezione di dati personali, soccombe rispetto alla tutela dell'onore e della reputazione (altrui)[93].

Nella ipotesi di attacco a siti *web*, con loro danno e relativa inutilizzabilità[94], si è ormai sempre più orientati a sacrificare il diritto all'anonimato (qualora venga invocato), riconoscendo la funzione sociale svolta da questi canali di comunicazione.

Stesso discorso nell'ipotesi di furto di identità, laddove la tutela alla propria identità personale ha il sopravvento su qualsiasi forma di anonimato che possa danneggiarla.

In conclusione, si può affermare che l'anonimato in Internet non può essere tutelato, laddove ci sia la necessità di identificare gli autori di condotte ingiuste e pregiudizievoli rispetto a diritti altrui e quindi ogni volta che ciò sia socialmente pericoloso. A differenza di quanto si possa pensare, il diritto tollera l'anonimato in rete, tanto da riconoscerlo come la "normalità" dell'attività dell'utente, ma subisce forti limitazioni nell'ipotesi di attività criminose. Sostanzialmente nel confronto tra il diritto alla *privacy*, la libertà di espressione (da leggere come anonimato) e la prevenzione del crimine "vince" la prevenzione del crimine.

[92] Per approfondimenti si rinvia all'interessante lettura dell'articolo di W. DAVIS, *Court: IP Addresses Are Not 'Personally Identifiable' Information*, su http://www.mediapost.com/publications/article/109242/.

[93] Cfr. E. PELINO, *L'anonimato su Internet*, cit., p. 293. Una categoria di limiti impliciti alla libertà di espressione conterrebbe diritti di eguale valore costituzionale, come: onore, riservatezza, ordine pubblico, prestigio del Governo e morale. In tal senso cfr. Corte Cost. 16 maggio 1962, n. 19, in "Giurisprudenza costituzionale", 1962, p. 189 e ss.

[94] Una pratica a volte effettuata per sfida, o per provocazione o ancora per contestazione politica, c.d. danneggiamento da *defacement* o da *Ddos attack* o *netstrike*.

In tal senso si può affermare che, più che l'anonimato puro, il diritto accetta un anonimato che potrebbe essere definito "relativo". Un anonimato, cioè, che riconosce a ciascuno il diritto di navigare in Rete "indossando una specie di maschera" solo previa identificazione presso gli intermediari della comunicazione. Una sorta di anonimato protetto che indirettamente conferma il principio dell'identificabilità. Sostanzialmente si può agire anche in forma anonima, ossia non in chiaro, purchè si permetta alle autorità competenti di essere rintracciati, ossia identificati in caso di necessità.

Gli unici soggetti a cui l'anonimato non è concesso sono gli ISP ai quali è preclusa la possibilità di nascondersi, celarsi o dissimulare la propria reale identità.

Il quadro normativo che disciplina e riduce il diritto all'anonimato in rete è rappresentato dalle norme collegate alla sicurezza informatica.

Nello stesso contesto si collocano: il "Codice della privacy" che nell'allegato B al punto 10 del Disciplinare Tecnico detta regole volte a proteggere la riservatezza del legittimo utente ma definisce anche la tracciabilità del dato; le normative antiterrorismo e la Direttiva 2006/24/CE. In tema di sicurezza e di procedure antiterrorismo, di cui il c.d. "Pacchetto Pisanu"[95] fu una conseguenza, si ricorda che il nostro legislatore già si era attivato con interventi precedenti al 2005. L'art. 226 disp. att. c.p.p., ad esempio, in tema di intercettazioni preventive volte a contrastare l'eversione ed il terrorismo internazionale e disposte ai soli fini investigativi e pertanto inutilizzabili nel procedimento penale, fu modificato dalla l. n. 438 del 2001.

Una sfaccettatura della *privacy* è il c.d. diritto all'oblio[96], da intendersi come la garanzia che determinate informazioni e/o notizie inerenti a procedimenti giudiziari o ad atti ufficiali, non siano continuamente riproposte oppure, decorso un certo periodo di tempo, queste non vengano più diffuse.

Il diritto all'oblio si colloca tra i diritti inviolabili della persona. I principali riferimenti normativi si ritrovano negli artt. 2 e 27, co. 3, Cost.

Recentemente ha fatto notizia il caso spagnolo del *Boletin Oficial de Estado*[97]. Alcuni cittadini spagnoli hanno contestato la digitalizzazione e la pubblicazione *on-line* del Bollettino, ricorrendo al Garante per la protezione dei dati personali, al fine di contrastare il pericolo di indicizzazione delle informazioni contenute nella pubblicazione da parte del motore di ricerca di

[95] L. n. 155 del 2005 "Misure urgenti per il contrasto del terrorismo internazionale".

[96] Cfr. M. MEZZANOTTE, *Il diritto all'oblio*, Napoli, ESI, 2009, *passim*.

[97] Corrispondente alla nostra Gazzetta Ufficiale in http://www.boe.es/.

Google che, di fatto, li avrebbe resi troppo facilmente reperibili. Il Garante ha riconosciuto legittima la richiesta.

In Italia ci sono stati due casi che hanno dimostrato, di fatto, l'altalenante posizione della giurisprudenza sulla materia: il caso "Mario Chiesa", nel quale è stato riconosciuto il diritto all'oblio[98] ed il caso "Giulio Caradonna"[99], conclusosi con una sentenza opposta e sfavorevole al riconoscimento di un diritto all'oblio.

Più recente è stata una decisione del Giudice monocratico del Tribunale di Chieti del 20 gennaio 2011[100], nella quale viene affermata la violazione della *privacy* (ed indirettamente un diritto all'oblio) favorevole ai ricorrenti che, pur non confutando la correttezza della notizia, hanno richiesto ed ottenuto la rimozione dell'articolo dalla testata *on-line*. La decisione ha evidenziato che gli archivi digitali sono, per loro stessa natura, più accessibili di quelli cartacei, permettendo così che la notizia possa essere continuamente riproposta, andando ben oltre il termine di ragionevole interesse pubblico.

Il diritto all'oblio, pur essendo un "prodotto" tipicamente giurisprudenziale, richiede una diretta ed esplicita disciplina normativa. In Italia sono stati presentati alcuni disegni di legge volti a regolamentare il fenomeno, ma ciò che si richiede è la previsione di un lasso di tempo ("variabile a seconda della gravità del reato") decorso il quale sia possibile o necessario rimuovere le immagini ed i dati, anche giudiziari, che consentano di identificare direttamente o indirettamente una persona indagata o anche "soltanto" imputata[101].

È bene ricordare che può sorgere una interferenza tra il diritto alla *privacy* e l'attività giudiziaria, con la possibilità di una forte limitazione della prima per ragioni di giustizia. Si verifica questa ipotesi ogni volta che

[98] L'articolo può essere consultato nella versione *on-line*, laRepubblica.it del 2 febbraio 2005 in http://ricerca.repubblica.it/repubblica/archivio/repubblica/2005/02/02/mario-chiesa-ha-diritto-all-oblio.html di Luca Fazzo.

[99] Tribunale di Roma del 19 gennaio 2004 che ha, indirettamente, negato un diritto all'oblio laddove sia presente una sorta di "diritto alla verità storica" qualora sia ben documentata, piuttosto che un vero e proprio diritto di cronaca. La sentenza è consultabile per esteso nel sito di Isole nella rete all'indirizzo http://www.ecn.org/inr/caradonna/sentenza.html.

[100] Il testo della sentenza è liberamente consultabile nel sito http://www.comellini.it/privacy_file/sent2011-8.htm.

[101] Sull'argomento si rinvia alla pubblicazione di M. SCHONBERGER, *Delete. The virtue of Forgetting in the Digital Age*, Princeton University Press, 2009. Cfr. inoltre G. SCORZA, *Il diritto all'oblio: caro web dimenticami*, del 12 gennaio 2010 in http://daily.wired.it. Sui progetti e disegni di legge presentati in questi ultimi anni si rinvia alla consultazione del sito del senato http://www.senato.it.; in proposito cfr. il disegno di legge c. 2455, XVI legislatura del 2009.

i dati personali del cittadino risultino correlati a vicende giudiziarie o a controversie[102].

Ci si pone, allora, il problema della raccolta della prova in modo che non violi tutte quelle ipotesi di divieto stabilite dalla norma perché altrimenti ne verrebbe vanificato l'utilizzo[103].

Il "Codice della privacy" prevede il "massimo riserbo" nel trattamento dei dati anche qualora sia effettuato per fini di giustizia ed in sede giudiziaria. È quanto stabilito negli artt. 24, lett. f)[104], e 132 del "Codice della privacy".

In proposito la l. n. 48 del 2008 sembra integrare "*dal punto di vista procedurale le modalità di accesso da parte delle forze dell'ordine ai dati di traffico conservati dagli operatori di comunicazione elettronica ai sensi dell'art. 132 del "Codice della privacy" (d.lgs. 196/03)*". L'articolo è stato modificato dal d.lgs. n. 109 del 2008 di recepimento della direttiva 24/06 sul fenomeno del già citato *data retention*[105].

L'art. 132, co. 4 *ter*, così come modificato, dovrebbe essere letto in combinato con l'art. 259 c.p.p., a sua volta riformulato, che contiene una dettagliata previsione di obblighi di custodia per i dati informatici sequestrati, onde impedirne l'alterazione o l'accesso da parte di terzi[106].

In realtà con questi interventi normativi il legislatore si è preoccupato, soprattutto, di assicurare il difficile equilibrio tra la tutela del soggetto a cui i dati si riferiscono e l'esigenza di operare in serenità da parte dell'Autorità competente nella fase delle indagini[107].

[102] Oltre alla già citata Direttiva 95/46/CE v. anche l'art. 47 d.lgs. 196 del 2003.

[103] Sull'inutilizzabilità cfr. in proposito l'art. 191 c.p.p. e P. TONINI, *Lineamenti di diritto processuale penale*, Milano, Giuffrè, 2010, p. 109 e ss. V., inoltre, A. BARGI, S. FÙRFARO, *Le intercettazioni di conversazioni e di comunicazioni*, in "La prova penale", Trattato diretto da A. Gaito, I, Torino, Utet, 2008, p. 165 e ss.

[104] Ossia quando il trattamento è necessario [...] ai fini dello svolgimento delle investigazioni difensive [...] o comunque per far valere o difendere un diritto in sede giudiziaria".

[105] Per ulteriori approfondimenti si rinvia a: V. ZENO ZENCOVICH, *Repressione della criminalità informatica e tutela dei diritti fondamentali*, cit.; S. ATERNO, A. CISTERNA, *Il legislatore interviene ancora sul data retention, ma non è finita*, in "Diritto penale e processo", Vol. 15, 2009, n. 3, p. 282 e ss.; C. CONTI, *Attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, in Lorusso S. (a cura di), "Le nuove norme sulla sicurezza pubblica", Padova, Cedam, 2008, p. 3 e ss.

[106] Cfr. l'ampia disamina di M.A. SENOR, *Legge 18 marzo 2008, n. 48 di ratifica ed esecuzione della Convenzione di Budapest sulla criminalità informatica: modifiche al codice di procedura penale e al d.lgs. 196/03*, in http://www.altalex.com/index.php?idnot=41576.

[107] Nella fase di acquisizione delle prove nel rispetto della genuinità delle fonti si può

Come già accennato gli interventi a livello europeo sono stati molti. Tra questi: la citata direttiva 2006/24/CE, recepita dal d.lgs. 30 maggio 2008, n.109, inerente il *data retention* ed, ovviamente, la pluricitata Convenzione di Budapest sulla criminalità informatica del 2001, la quale nel Preambolo, oltre a ribadire il diritto alla tutela dei dati personali, afferma: "la necessità di garantire un equilibrio adeguato fra l'interesse ad una azione repressiva ed il rispetto dei diritti umani fondamentali, come garantiti dalla Convenzione sulla protezione dei diritti dell'uomo e le libertà fondamentali del Consiglio d'Europa del 1950, il Patto internazionale su diritti civili e politici delle Nazioni Unite del 1966, nonché le altre convenzioni internazionali in materia di diritti umani le quali riaffermano il diritto a non subire ingerenze per le proprie opinioni, la libertà di espressione, compresa la libertà di cercare, ottenere e comunicare informazioni ed idee di ogni genere, senza limitazioni di frontiere, assieme al diritto al rispetto della vita privata"[108].

8. PROVA

"(...) tutto quello che non dirai non sarà usato contro di te"
Mel Gibson in "Arma Letale 3"

Appare ormai sempre più evidente quanto si sia evoluta la definizione di crimine informatico. Se in un primo momento con questo termine si intendeva il fenomeno criminale caratterizzato dall'abuso della tecnologia informatica (l'utilizzo della tecnologia informatica per compiere l'abuso oppure per realizzare il fatto criminoso), oggi ormai, si tende ad allargare tale

spaziare oltre il trattamento dati, così come previsto dal "Codice della privacy", toccando argomenti inerenti il divieto di pubblicazione di atti o immagini, l'obbligo al segreto previsti nel codice di procedura penale, *ex* artt. 114 e 115, e gli aspetti legati al diritto di cronaca. In tema di *privacy* si rinvia ai numerosi interventi del Garante della privacy, soprattutto in merito al *data retention*, cfr. in proposito il Comunicato stampa "Il garante ai gestori tlc: concernente le informazioni sulla navigazione in Internet, in http://www.garanteprivacy.it/garante/doc.jsp?ID=1481285.

[108] "In questa direzione si muovono le disposizioni riguardanti le violazioni della confidenzialità, l'integrità e la disponibilità dei dati e dei sistemi informatici ed in particolare l'art. 2 sull'accesso illegale, l'art. 3 sulle intercettazioni illegali, l'art. 4 sulla integrità dei dati, l'art. 7 sulla falsificazione dei dati, l'art. 8 sulle frodi informatiche, nonché una norma di chiusura, l'art. 15, il quale nel richiamare le sopra citate convenzioni internazionali, richiede che le misure sanzionatorie e procedurali siano rispettose del principio di proporzionalità", così V. ZENO ZENCOVICH, *Repressione della criminalità informatica e tutela dei diritti fondamentali*, cit., con riferimento al testo della Convenzione del Consiglio d'Europa sulla criminalità informatica 23 novembre 2001.

definizione ricomprendendovi "la presenza di una qualsiasi tecnologia informatica all'interno della scena del crimine" e la possibilità, o la necessità, di utilizzare questa tecnologia per fare chiarezza sull'evento criminale che si è verificato[109].

I crimini informatici potrebbero distinguersi in:

1. "crimini informatici con finalità di profitto" (per l'autore, con un conseguente danno nei confronti del soggetto che lo subisce) che comprendono i casi di appropriazione o manipolazione di programmi ed informazioni o le stesse frodi elettroniche;
2. "crimini informatici che hanno ad oggetto un computer" o un sistema informatico (è l'ipotesi del danneggiamento informatico) e, infine,
3. "crimini correlati all'uso del computer" laddove il computer, o la risorsa informatica in genere, si rivela utile/necessario per agevolare o per consumare una condotta illecita.

La novità dell'attività investigativa digitale sta nel fatto che l'informatica rappresenta una vera e propria disciplina, utilizzata per studiare l'insieme degli eventi legati al "caso" criminale. Utile, cioè, per analizzare e raccogliere le prove o anche solo per ricostruire i momenti determinanti dell'evento criminale.

La necessità di "operare" in un ambiente digitale, dove i crimini si concretizzano o possono essere ricostruiti così da riuscire a dedurre le motivazioni che spingono il soggetto a diventare un criminale, spinge l'investigatore a cercare di comprendere il complesso contesto in cui si trova proiettato.

L'Informatica forense[110] è una disciplina che si è guadagnata una propria autonomia a causa della forte specializzazione raggiunta[111]. Questo perché

[109] Gli strumenti informatici non rilevano più soltanto in occasione dei *computer crimes*, dei *cybercrimes* o dei *computer related crimes*, ma anche nei casi dei c.dd. reati comuni, come nell'ipotesi di omicidio (si pensi al "caso Rea"). Marco Strano, in un suo intervento alla Conferenza sul *Cyber crime* tenutasi a Palermo, 3-4-5 Ottobre 2002, poeticamente definì il cybercriminale come un individuo proiettato "in un contesto digitale, laddove la scena criminis [...] si localizza tra i polpastrelli dell'autore e la tastiera, tra i suoi occhi e le emissioni elettromagnetiche del monitor".

[110] Dalla tradizionale *computer forensic* si passa alla *digital forensic*, le cui linee guida furono segnate nel 2001 con il primo *Digital Forensic Research Workshop* (DFRWS, http://dfrws.org), ed ancora alla *Information Forensic*, alla *Network Forensic* ed alla *Mobile Forensic* o ancora alla *AntiForensic*, materia, quest'ultima, in cui oggetto di analisi è prevalentemente l'importanza della prova.

[111] Sull'informatica forense ed in special modo sulla *computer forensic* molto è stato prodotto. Per tutti cfr. L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, Giuffrè, 2007;

la scena del crimine è diventata anche digitale ed appare sempre più necessaria la figura di investigatori in grado di studiare la conservazione, identificazione, acquisizione, documentazione, protezione ed interpretazione dei dati presenti su un computer o veicolati attraverso la rete, così da poterli valutare come prove utili alla soluzione del "caso". Alcuni autori precisano la differenza tra *computer forensic* e sicurezza informatica[112] "seppure queste due aree siano strettamente collegate". Altri studiosi auspicano l'applicazione alla *computer forensic* di codici di condotta in grado di introdurre aspetti etici a cui gli investigatori, durante la propria attività, possono ispirarsi[113].

L'aggiornamento e la specializzazione nell'ambito di questa "materia" ha acquistato una importanza sempre più rilevante e sono molti i corsi (e relative certificazioni) universitari e no che si stanno facendo carico di questa particolare offerta formativa.

9. (CONTINUA) PROVA E COMPUTER FORENSIC. PROVA NEL/DEL REATO INFORMATICO

"Un giorno le macchine riusciranno a risolvere tutti i problemi,
ma mai nessuna di esse potrà porne uno"
Albert Einstein

La *computer forensic* nasce negli USA. Si è poi sviluppata in Europa. In Italia, nel 2003, un report della Commissione Europea[114] indicava la situa-

A. GHIRARDINI, G. FAGIOLI, *Computer forensics*, Milano, Apogeo, 2007, *passim*.

[112] G. COSTABILE, *Computer forensic e informatica investigativa alla luce della l. n. 48 del 2008*, in "Cyberspazio e diritto", 2010, vol. 11, n. 3, p. 465 e ss. riconduce la sicurezza informatica alla *antiforensic* che per sua natura è rivolta ad occultare i dati e vanificare o comunque rendere più difficoltoso l'operato degli investigatori. In proposito si rinvia ai numerosi contributi sullo specifico argomento che, forse per il suo "lato oscuro" affascina particolarmente. Tra gli esperti che da sempre operano sul campo cfr. l'incessante attività di D. Gabrini (*alias Rebus*), con il suo sito www.tipiloschi.net, in cui è possibile consultare materiale utile, tra questo si rinvia alla lettura della sua lezione "Introduzione alla computer forensic", Pavia, 14-06-2011.

[113] L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica*, cit., p. 25 e ss. Per l'applicazione di codici etici cfr. Codice etico dell'associazione IISFA consultabile alla www.iisfa.net.

[114] Così il CSIRTs, ossia il *Computer Security Incident Response teams* (in italiano: Gruppo di gestione degli incidenti di sicurezza informatica) ed il suo studio *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries* in http://ec.europa.eu/information_society/eeurope/2005/all_about/security/handbook/index_en.htm. Sulla storia ed evoluzione dei CIRSTs t si rinvia all'esauriente Documento della Enisa (l'agen-

zione in tema di *computer forensic* come una «*still at an early developed stage*» (ancora ad uno stadio di sviluppo iniziale) in cui gli organi investigativi e quelli giudicanti ancora non avevano ben chiara una corretta metodologia dell'acquisizione della prova digitale, concentrandosi e rimanendo ancorati ad un diritto penale sostanziale di tipo tradizionale.

In realtà, è bene ricordare che in Italia i primi tentativi di creare team di esperti ci sono stati già nel 1989, con l'istituzione di un gruppo di specialisti in seno alla Direzione Centrale della Polizia Criminale, il cui compito era di analizzare la criminalità legata al settore delle telecomunicazioni[115].

Tra continue evoluzioni si è arrivati alla creazione della Polizia Postale e delle Comunicazioni, istituita nel 1998[116] e composta da circa 2000 persone che svolgono la loro attività attraverso unità specializzate, distribuite sull'intero territorio nazionale 19 Compartimenti regionali e 77 Sezioni provinciali[117]), e coordinate dal Servizio centrale.

Nel 2001 è stato istituito il GAT - Gruppo Anticrimine Tecnologico della Guardia di Finanza[118].

Sono operativi, inoltre, i vari Reparti di Investigazioni Scientifiche - RIS dei Carabinieri con le loro Sezioni specializzate come la Sezione Telematica del Reparto Tecnologie Informatiche - RTI operante all'interno del RaCIS -

zia dell'UE per la sicurezza informatica http://www.enisa.europa.eu/), WP2006/5.1(CERT-D1/D2). Si riporta la definizione che viene data dei CSIRST: "Un CSIRT è un gruppo di esperti in sicurezza IT, la cui attività principale consiste nel reagire a incidenti di sicurezza informatica. Esso fornisce i servizi necessari per affrontare tali incidenti e aiutare i relativi utenti di riferimento a riprendersi dalle violazioni.

[115] E con l'intento di monitorare e controllare i movimenti di stampo mafioso.

[116] Con Decreto del Ministro dell'Interno del 31 marzo 1998 e la cui attività si rivolge alla prevenzione ed al contrasto della criminalità informatica attraverso il "raggiungimento di due fondamentali obiettivi: la protezione delle "infrastrutture tecnologiche" che, sulla Rete, assumono una valenza strategica per la sicurezza e la prosperità del Paese; la protezione degli "utenti" della Rete e dei valori che gli stessi, quotidianamente, affidano all'infrastruttura telematica ai fini della loro soddisfazione." Così D. VULPIANI, *La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto*, in "Rivista di Criminologia, Vittimologia e Sicurezza", Vol. 1, 2007, n. 1, p. 2.

[117] Dati riferiti da D. VULPIANI, *La nuova criminalità informatica*, cit., p. 5. Altri corpi specializzati nel settore sono: il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche Informatizzate (CNAIPIC) ed il Centro Nazionale per il Contrasto della Pedofilia, l'adozione del *Child Exploitation Tracking System* - CETS nato per contrastare la pedofilia *on-line*.

[118] Ora Nucleo Speciale Frodi Telematiche http://www.gat.gdf.it.

Raggruppamento Carabinieri Investigazioni Scientifiche[119].

La collaborazione è presente sia a livello nazionale (Ministero delle Comunicazioni e la stessa Authority per le garanzie nelle Comunicazioni) sia a livello internazionale (Gruppo ad Alta Tecnologia del G8[120], UE, OCSE, EUROPOL[121], INTERPOL, Consiglio d'Europa[122]).

A livello transnazionale ci sono stati diversi casi di collaborazione tra le autorità giudiziarie e di polizia dei vari Stati. Ad esempio nella lotta alla pornografia infantile la "collaborazione" fra gli organi di contrasto alla criminalità statunitensi ed europei (USA e Germania) si è rivelata vincente. Uno degli ultimi casi ha riguardato la scoperta in Internet da parte di alcuni cyberpoliziotti tedeschi di siti coinvolti nella distribuzione di materiale pornografico minorile i cui destinatari erano residenti negli USA. Un "cittadino vigile" segnalò, all'epoca, ai poliziotti tramite *e-mail* un sito *web* contenente disegni che mostravano minori in pose "erotiche". La segnalazione fu inoltrata dal BKA tedesco (Ufficio Federale penale anticrimine) ai colleghi USA,

[119] Per ulteriori informazioni cfr. il sito http://www.carabinieri.it/Internet/Arma/Oggi/RACIS/.

[120] Nel marzo del 1998 il Consiglio europeo ha proposto l'istituzione di una rete preposta allo scambio di informazioni contro la criminalità ad alta tecnologia nell'ambito del G8. Alla rete hanno aderito Australia, Brasile, Canada, Danimarca, Finlandia, Francia, Germania, Italia, Giappone, Paesi Bassi, Russia, Spagna, Svezia, Regno Unito e Stati Uniti d'America. Nel 2001 è seguita la Convenzione di Budapest sul Cybercrime. Cfr., inoltre la Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni - Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica - eEurope 2002 /* COM/2000/0890 def. */ in http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52000DC0890:IT:HTML, redatta a tutela della sicurezza delle reti e contro la criminalità telematica e nata con l'intento di "agire per prevenire le attività criminali sia aumentando la sicurezza delle infrastrutture dell'informazione sia facendo in modo che le autorità preposte all'applicazione della legge dispongano di opportuni strumenti d'intervento, nel pieno rispetto dei diritti fondamentali dei cittadini".

[121] Sull'Europol, sulla sua nascita, la sua struttura e sul quadro giuridico ed istituzionale, si rinvia alla dettagliata serie di notizie contenute nel Documento conclusivo dell'indagine conoscitiva sulle potenzialità e le prospettive di Europol, Comitato parlamentare Schengen, Europol e immigrazione, in http://www.camera.it/_bicamerali/leg14/schengen/indaginiconoscitive/doc290103.htm.

[122] Cfr. in proposito la Comunicazione relativa alla protezione delle infrastrutture critiche informatizzate "Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale" del 31 marzo 2011, in http://www.parlamento.it/web/docuorc2004.nsf/8fc228fe50daa42bc12576900058cada/8fed05cad2c7e6f3c1257865003ab37a/$FILE/COM2011_0163_IT.pdf.

l'ufficio dogana statunitense e l'FBI svolsero le indagini per oltre un anno, concludendole con l'arresto di due cittadini statunitensi nella Louisiana.

Hanno fatto scuola altri due vecchi casi[123] risolti grazie alla collaborazione tra l'FBI statunitense e la polizia inglese. Uno ha riguardato un attacco informatico concretizzatosi negli USA ed in cui i pirati informatici erano riusciti a violare le pagine *web* di alcuni *server* governativi, tanto da costringere a isolarne alcuni dalla Rete. Tra questi il sito *web* del Senato che fu preso di mira da un gruppo denominato MOD (*Masters of Download* - Maestri del download), i cui appartenenti non erano cittadini USA e che, dalle tracce informatiche risultavano residenti in Gran Bretagna. L' altro caso si concluse con l'arresto di uno studente indonesiano, residente nei dintorni di Bonn, che, riuscì a collegarsi ad un fornitore di servizi Internet a Miami, scaricando sul proprio computer ben 11.000 numeri di carte di credito. Al suo ricatto (restituzione dei numeri in cambio di "soli" 30.000 dollari) il *provider* americano si rivolse alla polizia e questa a sua volta ai servizi segreti che, insieme al BKA, riuscirono ad identificare e quindi catturare il mittente del messaggio ricattatorio.

A livello europeo, soprattutto alla fine degli anni novanta, si è sviluppata una vera e propria sensibilizzazione sul tema. Molti i progetti e le collaborazioni che presero vita. Tra queste: il progetto "Enfopol 98", con l'intento di controllare Internet[124] ed il progetto elaborato dal Gruppo di lavoro del G8, durante una riunione a Parigi, basato sulla tecnica del "congelamento e successiva memorizzazione" dei dati raccolti, in previsione della stesura di una metodologia condivisa per l' acquisizione delle prove digitali.

10. Analisi forense. Best practices. Ispezione e sequestro

"Il computer non è in grado di trasmettervi il lato emozionale della questione.
Può fornirvi la matematica, ma non le sopracciglia"
Frank Zappa

[123] *Alla ricerca di tracce sulla rete* (dossier pubblicato su "Süddeutsche Zeitung" dell'8 giugno). Il caso, datato 1999, è citato dal Garante della privacy nella Newsletter 14-20 giugno 1999, in http://www.garanteprivacy.it/garante/doc.jsp?ID=48603.

[124] E perciò fu visto come la versione europea di Echelon ed osteggiata in tutti i modi per il forte impatto con le libertà civili dei cittadini. Sull'argomento v. l'interessante articolo apparso su Punto Informatico del 28 luglio 2000, di F. Boccazzi Varotto, *ENFOPOL si sa ma non si dice*, in http://punto-informatico.it/6585/PI/Commenti/enfopol-si-sa-ma-non-si-dice.aspx.

"articoli/devivo" — 2012/4/5 — 10:45 — page 80 — #80

L'"analisi forense" consiste nel ricercare e raccogliere (repertare) le prove digitali con l'intento di analizzarne i contenuti e capire se questi sono leciti oppure no, successivamente utilizzarle in un contesto legale. Non si esaurisce in ambito legale, dove l'avvocato e/o l'operatore giuridico utilizzano ed esibiscono prove digitali, ma può esplicarsi anche in un ambito extragiudiziario (o anche pre-giudiziario) come ad esempio quello aziendale, laddove siano presenti dati digitali che possono diventare oggetto di incidenti informatici[125]; ossia possono diventare oggetto di un morboso ed illecito interesse di individui non autorizzati a trattarli o a conoscerli.

Per prova digitale si intende "qualsiasi dato memorizzato o trasmesso usando un computer che supporta o respinge una teoria su come è avvenuto un fatto offensivo o che individua elementi critici dell'offesa, come l'intenzionalità o l'alibi"[126]. Potrebbe estendersi, dunque, sia allo strumento usato sia al supporto in grado di conservare le prove di un illecito (con relativa possibilità di identificarne l'autore). Inoltre, come già accennato, questi strumenti informatici mantengono traccia di reati non soltanto informatici e diventano elementi in grado, di volta in volta, di accertare il reato o di raccoglierne le prove diventando, laddove non sono corpo del reato, strumenti pertinenti ad esso[127].

[125] Per incidente informatico si può intendere sia un attacco informatico, consistente nella violazione o nel "deturpamento" di un sito oppure di un archivio di dati, sia la perdita di dati (sovrascrittura di un documento, cancellazione di una *directory*, *backup* errato).

[126] La definizione è riportata da L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra processo scientifico e garanzie fondamentali*, Milano, Giuffrè, 2007, p. 60.

[127] Mentre la definizione di "corpo del reato" è espressamente prevista dal nostro legislatore nell'art. 253 c.p.p. ricomprendendovi sia i *corpora delicti* sia i *producta sceleris* (cose in rapporto diretto ed immediato con l'azione delittuosa), le c.dd. "cose pertinenti" al reato non hanno una precisa definizione normativa. Resta pertanto la genericità della definizione, dovuta alla stessa "natura" della *res* che in tal caso è indirettamente legata alla fattispecie concreta e perciò strumentale all'accertamento dei fatti, secondo i parametri che si rifanno al principio della libera prova e del libero convincimento del giudice. In pratica vengono ritenute "pertinenti" quelle cose che, anche indirettamente, sono utili a dimostrare sia il reato sia le modalità di preparazione ed esecuzione dello stesso ed inoltre risultino necessarie per la conservazione delle tracce e per l'identificazione dell'autore del reato. Sostanzialmente quelle cose che possono contribuire alla determinazione e comprensione dell'*ante factum* e del *post factum* perché ricollegabili al reato. Cfr. inoltre F. CORDERO, *Procedura penale*, Milano, Giuffrè, 2003, p. 83, che definisce "pertinente al reato ogni reperto utile a convinzione o a discolpa", ricomprendendo in questa espressione un reperto in grado di dimostrare: il reato, le sue modalità, l'accertamento del movente, tutti i movimenti collegati al reato (prima e dopo il suo evento) o, in caso di particolare fortuna per l'investigatore, l'identità del colpevole.

La *digital evidence* pur consistendo in qualsiasi informazione memorizzata o trasmessa in formato digitale, conserva la sua funzione di "memoria"[128], pertanto è sottoposta allo stesso regime di ricerca, raccolta, repertamento e corretta analisi previsto per la prova c.d. "tradizionale".

È, perciò, opportuno ricordare che quando si parla di prova, e dunque della "incorporazione" di un fatto in un supporto, è relativamente importante che questa risieda in un elemento materiale oppure non materiale (ad esempio in un foglio scritto oppure in un *file*) perché ciò non ne altera la natura (di prova, appunto).

In linea con la tradizionale indagine di una scena *criminis*, si potrebbe parlare di analisi forense *post-mortem*, facendo riferimento ad analisi su sistemi informatici (o computer) "a macchina spenta", dopo che si è verificata una intrusione o un illecito; oppure di una *live forensic analisys* ("in vita") qualora si operi su sistemi attivi colpiti da attacchi che hanno ad oggetto dati in memoria che si perderebbero con lo spegnimento del dispositivo.

La *digital evidence* è, in realtà, una *species* del *genus* della prova scientifica, con caratteristiche proprie, quali l' immaterialità e (di conseguenza) l'alterabilità. Un'alterabilità che, peraltro, è del tutto indipendente da intenti dolosi o colposi di terzi[129]. La prova informatica, oltre ad essere alterabile, è di per sé rumorosa[130] ed anonima. Per ridurre al minimo una sua possibile contaminazione è previsto l'uso di applicazioni specifiche ossia di particolari tipi di *tools*. L'antiforensic consiste proprio in tecniche che mirano ad inibire i *tools* o a confonderli, così da rendere particolarmente difficoltoso l'operato dell'analista.

La *e-digital* può essere prodotta dall'uomo (ad esempio una *e-mail*), oppure può essere creata autonomamente dal computer (ad esempio un *file* di *log* o un *cookie*) o, infine, può essere predisposta dall'uomo e dal computer congiuntamente (ad esempio un foglio excel).

L'attività investigativa della polizia giudiziaria si confronta con queste scie informatiche non solo nel tentativo di ricostruire attraverso i supporti infor-

[128] Da un punto di vista civilistico: "Attraverso tale strumento, invero, la parte ha la possibilità di suffragare la propria domanda o eccezione ed imporre, in questo modo, quella riproduzione della realtà passata che sia consona alla posizione giuridica fatta valere in giudizio", così M. CONTE, *Le prove civili*, Milano, Giuffrè, 2009, p. 47.

[129] Si pensi alla quotidiana prassi di colui che lavora sistematicamente con il proprio pc e che alla semplice apertura di un *file* altera, pur non volendo, i dati inerenti alla data ed all'orario di accesso del *file*.

[130] Rumorosa per la mole di dati di cui è composta e che debbono essere analizzati.

matici le potenziali tracce del reato, ma anche nella necessità di acquisire tali "tracce" in modo corretto ed ineccepibile per la fase dibattimentale e, dunque, anche rispettando tutte quelle regole di reperimento che siano in grado di preservarle fino al momento della loro analisi, soprattutto qualora non sia possibile effettuare gli accertamenti direttamente *in loco*.

Lo scopo dell'Informatica forense, infatti non si esaurisce nell'evitare che si verifichino "impatti" inquinanti sulle prove, ma anche nel documentare puntigliosamente ogni intervento di raccolta delle stesse, così da prevenire contestazioni sulla autenticità dei reperti e sulla loro asettica potenziale ricostruibilità della situazione esaminata.

Le fasi di formazione della prova informatica consistono: a) nella sua individuazione (con conseguente ispezione oppure sequestro), b) nell'acquisizione, che è la fase più delicata, c) nella analisi ed infine d) nella valutazione.

Il repertamento digitale[131] si suole distinguere in due fasi: "il repertamento dell'oggetto fisico, che mantiene i dati seguendo un qualche principio fisico (in genere elettrico, magnetico e/o ottico); ed il repertamento dei dati ossia la fedele copia dei dati su supporto sicuro"[132].

La l. n. 48 del 2008 è stata determinante, ma non completamente chiara ed esaustiva per quanto riguarda l'elencazione di alcune delle garanzie introdotte per i mezzi di ricerca della raccolta delle prove informatiche, riassumibili, brevemente, in pochi punti:

1. conservazione ed inalterabilità dell'originale informatico così da poterne garantire la sostanziale genuinità;
2. impedimento di qualsiasi forma di alterazione successiva del dato originale;
3. obbligo di creare una copia conforme all'originale del dato informatico acquisito;
4. obbligo di assicurare la immodificabilità di detta copia;
5. garanzia della installazione di eventuali sigilli "informatici" sui documenti acquisiti.

[131] "Si stanno diffondendo rapidamente sistemi portatili di repertamento dati che consentono di clonare il contenuto completo o parziale di un pc senza necessariamente prelevarlo e trasportarlo in un laboratorio specializzato e questo mentre continua a funzionare (*live analysis*). Tale dualità tra fisico e dato si presenta solo nella digital forensics ed in nessun altra materia scientifica forense" così M. MATTIUCCI, *Digital forensic*, in http://www.aserc.it.gg/Digital-Forensic.htm.

[132] M. MATTIUCCI, *Op. cit.*, *sub* 131.

"articoli/devivo" — 2012/4/5 — 10:45 — page 83 — #83

È possibile, inoltre, elaborare, in base all'esperienza acquisita "sul campo", una sorta di protocollo ancora più ampio, che riguardi non solo la fase del repertamento delle prove digitali[133] inerenti il reato avvenuto, ma anche la fase volta a prevenire o a contrastare il reato[134].

Nel quadro generale in cui collocare il corretto espletamento di ricerca della prova informatica[135] "il supporto informatico deve considerarsi autonomo rispetto al documento digitale" e, pertanto, "questo principio di autonomia influisce anche sui mezzi di ricerca della prova informatica che necessitano di una apposita regolamentazione, oggi in larga parte tracciata dalle norme del codice così come sono state modificate dalla legge n. 48 del 2008"[136].

In realtà la carenza di un documento ufficiale contenente le "Linee guida" per le indagini digitali è stata fatta notare da più parti ed in varie occasioni. Nella ipotesi di *criminal evidence*, infatti, il nostro ordinamento sembra recepire passivamente una prassi anglo-americana che vede il giudice in veste di vigilante del rispetto delle nuove metodologie di accertamento tecnologico[137].

La necessità di *standard operating procedure* idonee a garantire correttezza ed autenticità nell'accertamento, ha incoraggiato la compilazione di (ottimi) decaloghi, creando, una *best practices*[138] a cui è possibile fare riferimento.

I punti salienti potrebbero essere sintetizzati in alcune regole essenziali[139].

[133] Ricerca e raccolta delle prove nonché loro conservazione per una corretta esibizione in fase dibattimentale.

[134] Attività che spesso viene svolta "in copertura".

[135] Appartengono alla fase del repertamento tutte quelle procedure che riguardano l'acquisizione di un pc e delle memorie di massa; il trattamento di un *server*, di un PDA oppure di un cellulare o di un sistema in rete, oppure di quelli che vengono definiti sistemi speciali e così via.

[136] P. TONINI, *Manuale di procedura penale*, Milano, Giuffrè, 2010, p. 366 e s.

[137] L. LUPARIA, *Computer crime*, cit., p. 383.

[138] Cfr., fra i numerosi contributi a livello internazionale, B. NELSON, A PHILLIPS, F. EFFINGER, *Guide to Computer Forensic and Investigations*, 2007, *passim*.

[139] Il corsivo riportato nel testo è tratto dall'interessante contributo di M. MATTIUCCI, *Digital Forensic*, in http://www.marcomattiucci.it/reper.php (data di consultazione: dicembre 2011); cfr. inoltre, dello stesso autore, quanto pubblicato in http://www.aserc.it.gg/Digital-Forensic.htm a cui si rinvia per ulteriori approfondimenti (data di consultazione: dicembre 2011). Cfr. anche, soprattutto per quanto riguarda la procedura di analisi della fonte di prova digitale, L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica*, cit., p. 63 e ss.

Repertamento di pc e di memorie di massa: l'indicazione fondamentale è quella di non "smanettare" direttamente sul sistema alla ricerca di dati utili nella fase di sopralluogo. La prima operazione da compiere è la disattivazione del sistema. Questo perché l'unico stato dell'elaboratore che assicura la sua impossibilità di proteggersi o distruggere dati utili è proprio quello in cui la circuiteria non è alimentata elettricamente.

Raccolta dell'*hardware* e documentazione della sua configurazione: prima di smontare i vari componenti del computer, è importante che vengano fatte delle fotografie dello stesso da varie angolazioni per documentare la configurazione *hardware* e le relative connessioni. Una volta smontato il sistema si abbia cura di imballare le singole parti in contenitori che diano la sufficiente protezione meccanica.

Raccolta dei supporti di memoria di massa: dopo la disattivazione del sistema (che deve necessariamente essere svolta via *hardware* e non via *software*) individuato è necessario passare a raccogliere fisicamente tutti si supporti di memorizzazione presenti.

Documentazione dei supporti magneto-ottici di memoria individuati: *floppy disk*, CD, cassette e nastri magnetici di vari formati sono una fonte di dati il più delle volte importantissima ai fini del repertamento, quindi è necessario soffermarsi accuratamente a catalogare ed etichettare tutto il materiale di tal tipo.

Trasferimento del materiale repertato in un luogo sicuro: un computer o una memoria di massa, una volta sequestrati e prima dell'analisi dei dati, devono essere conservati come reperti e quindi in un luogo poco accessibile, regolato termicamente e tracciato negli ingressi.

Repertamento dei *server*: raramente è indicato effettuare un repertamento fisico di un *server*, sia per la difficoltà nell'isolare e spegnere correttamente un tale tipo di strumento (generalmente operante real time in rete) che per l'eventuale danno che si finirebbe per arrecare all'organizzazione che lo possiede. La modalità essenziale quindi è quella di individuare i dati di interesse e clonarli in maniera irripetibile (presenza dei periti di parte art. 360 CPP). In alcuni casi è anche possibile effettuare un backup completo del sistema (se i dati sono in quantità limitata). Si tratta di un approccio più sicuro in relazione all'indagine ma preoccupante dal punto di vista della liceità del prelievo (= sequestro) di una mole di dati tanto varia e spesso non strettamente inerente il procedimento penale.

Repertamento dei PDA e dei cellulari: i *palmtop* e gli *smartphone* sono sor-

genti di dati generalmente insostituibili per le indagini. Purtroppo il loro repertamento non è immediato, soprattutto se il sistema gestisce servizi di comunicazione cellulare. Devono essere prese precauzioni sia per isolare le comunicazioni radio che per impedire lo spegnimento del dispositivo (*Mobile Forensics*).

Trattamento di un sistema in rete: problematica tipica dei *server* e spesso anche di pc casalinghi sui quali si interviene "a caldo" durante le comunicazioni su Internet. Non esiste, ad oggi e per quanto in mia conoscenza, una metodologia generale che preservi tutte le informazioni (quelle in RAM sono in questo caso fondamentali) e che riduca a zero l'intrusività. Da questo punto di vista l'unico modo per effettuare una sorta di repertamento dati è forzare un *logging* dell'attività della macchina mediante dei *software* che non necessitano di installazione, il tutto "live", ossia senza spegnere nulla. A ciò sarebbe opportuno aggiungere una video camera che riprende le attività sviluppate dall'operatore forense (per la sua migliore tutela legale).

Repertamento di sistemi video/fotografici: videocamere e macchine fotografiche digitali devono essere repertati nell'ambito High Tech, soprattutto tenendo conto che le memorie interne/removibili che possiedono su mini schede o *chip* possono contenere *file* di qualsiasi genere e non necessariamente immagini. Il prelievo di tali sistemi è relativamente semplice dato che le loro memorie sono in massima parte non temporanee. Bisogna fare molta attenzione a prelevare tutte le memorie effettivamente presenti sulla scena del crimine che talvolta possono passare inosservate data la minima dimensione e magari la lontananza dal sistema di ripresa foto/video.

Repertamento di *smartcard* e sistemi correlati: le *smartcard* vengono impiegati in diversi settori, dalla telefonia mobile all'identificazione biometrica. I lettori e modificatori di *smartcard* sono generalmente dei sistemi *special purpose* simili a pc per cui il loro repertamento segue quanto visto in precedenza. La *smartcard* può essere prelevata senza problemi a patto che non risulti in attività su una di tali macchine.

Repertamento di *magnetic-card* e sistemi correlati: le *magnetic card* trovano il massimo impiego nelle carte di pagamento ed identificazione. Anche in questo caso i lettori/scrittori di *card* sono dei sistemi *special purpose* simili a pc e talvolta solo pc collegati a speciali periferiche (es. *skimmer*). Il loro repertamento, quindi è sostanzialmente di prassi.

Repertamento di sistemi speciali: i sistemi elettronici speciali come GPS,

detonatori, microspie, ecc. necessitano di un repertamento altamente specialistico non suscettibile di generalizzazioni teoriche.

Le *Guidelines for Evidence Collection and Archiving*[140], contenute nel RFC 3227, rappresentano ancora oggi, a detta degli esperti, un documento più che valido a livello internazionale, pur essendo stato redatto nel 2002.

In esso vengono indicate le procedure più corrette e meno invasive da attuare nella raccolta delle prove. Ad esempio: procedere nella raccolta in considerazione della volatilità degli strumenti analizzati; prestare sempre attenzione onde evitare atteggiamenti non adeguatamente asettici sul luogo della raccolta delle prove; rispettare la *privacy*; rispettare determinate procedure sia nella raccolta sia nell'archiviazione; dettagliare minuziosamente tutto ciò che viene espletato nella fase della raccolta delle prove e descrivere la *scena criminis* in ogni minimo dettaglio cosicché possa testimoniare con esattezza, anche dopo anni, l'evento criminoso.

Una particolare attenzione viene riservata anche a quella procedura chiamata "Catena di custodia" (c.d. *chain of custody*) che regola minuziosamente lo stato del reperto durante i vari passaggi fisici ed informatici. Fa parte di questa procedura la descrizione chiara di come è stata trovata la prova, di come è stata "gestita" e di tutto ciò che le è accaduto. Sostanzialmente tutto si riduce a come sono state e vengono trattate le prove: "dove, quando e da chi sono state scoperte; dove, quando e da chi sono state trattate ed esaminate; chi ne ha preso la custodia, per quanto tempo ed in quale periodo; come sono state memorizzate; se e quando le prove hanno cambiato custodia; quando e come ciò è stato fatto; limitare gli accessi ad esse" ecc.[141].

Oltre oceano il NIST - National Institute of Standards and Technology che è un'agenzia del governo degli USA e si occupa della gestione delle tecnologie, ha provveduto a compilare altre linee guida[142].

In Inghilterra la ACPO - Association of Chief Police Officers[143] ha stilato le *Computer based evidence* ossia le linee guida inglesi per la raccolta e la

[140] Per il testo cfr. http://www.faqs.org/rfcs/rfc3227.html.

[141] Dalla traduzione del documento.

[142] Diverse a seconda delle tecnologie analizzate: la *Guide to Integrating Forensics Techniques into Incident Response*, in http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf, del 2006; la *Guidelines on Cell Phone Forensics*, in http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf del 2007 e la *Guidelines on PDA Forensics* in http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf del 2004.

[143] http://www.acpo.police.uk/.

conservazione della prova informatica[144].

Sostanzialmente le linee guida da rispettare in una indagine digitale riguardano: la fase corrispondente all'acquisizione delle prove; la fase del rispetto dell'inalterabilità delle stesse[145]; la fase della garanzia dell'originale alla copia, ossia volta ad assicurare che le prove eventualmente trasferite su altro supporto siano identiche a quelle originarie[146]; la fase dell'analisi delle prove, da svolgersi senza che vi siano pericoli di alterazioni.

In riferimento alla fase iniziale, ossia quella riguardante l'acquisizione delle prove, spesso il ricorso al sequestro appare inevitabile, ma occorre chiarire che questo pur rappresentando lo strumento più immediato e sicuro, non sempre può essere attuato con facilità, soprattutto laddove si opera in un ambiente digitale e non tutti i dati possono essere acquisiti fisicamente.

Per quanto riguarda le due fasi successive (inalterabilità e garanzia) è essenziale la dimostrazione che tra copia ed originale vi sia totale identità. La dimostrazione deve assicurare equivalenza ed indistinguibilità tra i dati originali ed i dati copiati, per tutta la fase del procedimento. "La copia deve essere, a livello logico, perfettamente identica al dispositivo originale. Dovranno essere preservati quindi non solo i dati, ma anche lo spazio libero sul disco, i metadati, il *master boot record*, ecc."[147] utilizzando la tecnica del *bit stream image*. Tutto ciò deve inoltre risultare sia in caso si effettui un sequestro senza il prelievo del bene informatico sia nell'ipotesi di una semplice ispezione.

La particolare attenzione riservata alla procedura discende dal rispetto del principio generale del "giusto processo" in cui si riconosce all'imputato il diritto a confrontarsi con il dato informatico "nel suo aspetto genuino, senza alterazioni". In sostanza il diritto a confrontarsi ad armi pari con l'accusatore[148].

[144] Il file è consultabile in .pdf nel sito di Ictlex, http://www.ictlex.net/wp-content/gpgcomputerbasedevidencev3.pdf.

[145] Ad esempio nel caso in cui sia coinvolto un sistema informatico l'acquisizione delle tracce deve essere svolta senza modificare il sistema stesso. Cfr. quanto indicato sopra.

[146] Si parla della c.d. copia forense che permette di acquisire una immagine *bit-stream* (una duplicazione *bit* a *bit* del supporto oggetto dell' indagine). Cfr. G. COSTABILE, *Scena criminis, documento informatico e formazione della prova penale*, in "Diritto dell'informazione e dell'informatica", 2005, n. 3, p. 531.

[147] G. COSTABILE, *Computer forensic e informatica investigativa*, cit., p. 499.

[148] P. TONINI, *Documento informatico e giusto processo*, in "Diritto penale e processo", Vol. 15, 2009, n. 4, p. 406.

Spesso si sceglie di optare per l'ispezione al posto del sequestro, questo perché l'ispezione avrebbe un minore impatto sulla quotidiana attività del soggetto proprietario dello strumento informatico oggetto dell'indagine. Si pensi al caso in cui il computer rappresenti lo strumento prevalente di lavoro. È bene ricordare che l'ispezione svolta dalla polizia giudiziaria è finalizzata all'esame dei luoghi o delle persone per accertare se vi siano tracce del reato. Per quanto riguarda l'opportunità di utilizzare uno strumento al posto dell'altro si rinvia ad approfondimenti di "settore"[149].

Accade sempre più spesso, nell'ipotesi del sequestro, di lasciare il materiale repertato in custodia giudiziale presso chi lo detiene. Ciò al fine di evitare, per quanto possibile, richieste di risarcimento danni degli apparati (che potrebbero danneggiarsi durante il trasporto o la semplice custodia presso gli uffici giudiziari) e facilitare tutte quelle operazioni legate ad un successivo dissequestro.

11. Responsabilità per violazione delle best practices

"Ogni problema ha tre soluzioni:
la mia soluzione, la tua soluzione e la soluzione giusta"
Platone

La fase finale che riguarda l'utilizzo degli strumenti probatori in giudizio è particolarmente delicata perché volta a valutare il materiale raccolto, controllando le prove acquisite ed interpretandole nel modo più oggettivo possibile, attraverso ricostruzioni e correlazioni. Il fattore umano, in questa fase, prende il sopravvento, riacquistando il suo ruolo originario.

Non si deve dimenticare che l'ambiente digitale in genere e lo strumento informatico in particolare hanno un'"alta potenzialità offensiva" e consentono di nascondere o cancellare facilmente gli elementi probatori. Tutto ciò ri-

[149] Cfr. in tal senso A. Scalfati, *Trattato di procedura penale*, II, 2009, Torino, Utet, spec. p. 400 e ss. e p. 437 e ss.; P. Tonini, *Manuale di procedura penale*, cit., il quale rileva come la stessa l. n. 48 del 2008 abbia ricondotto tra i mezzi "tipici" di ricerca della prova anche le ispezioni ed i sequestri operati su strumenti-sistemi o supporti informatici (p. 367). Per ulteriori approfondimenti in merito al sequestro e/o alla masterizzazione di materiale informatico e delle impronte elettroniche cfr. S. Aterno, *In materia di sequestro di hd e acquisizione della prova informatica: un caso eclatante*, nota a Trib. Milano 11 marzo 2005, in "Diritto dell'Internet", 2005, n. 4, p. 365 e ss. e G. Costabile, *Computer forensic e informatica investigativa*, cit., p. 472 e s. Fermo restando che in alcune ipotesi, come ad esempio pedopornografia digitale e violazione del diritto d'autore, il sequestro del materiale informatico è ritenuto insostituibile.

vela quanto sia determinante la tempestività nella denuncia e nell'intervento dell'autorità giudiziaria.

Il rispetto delle *best practice* e l'ipotesi di una loro violazione nella fase del repertamento apre un discorso ulteriore inerente l'attendibilità delle prove informatiche. Infatti, la conseguenza di una "maldestra acquisizione di una digital evidence durante le indagini" potrebbe compromettere la solidità della prova, rendendola inaffidabile.

Per una parte della dottrina non può condividersi l'opinione "secondo cui la mancata adozione delle migliori pratiche di digital forensic conduca alla nullità del mezzo di ricerca della prova" e neanche "nella sanzione processuale dell'inutilizzabilità" ma semmai "L'inosservanza delle misure tecniche idonee ad assicurare la salvaguardia della genuinità dei dati e delle informazioni raccolte si risolve sotto il profilo della valutazione della prova ed in particolare sul crinale della fondatezza dei risultati acquisiti" al punto che "Se la raccolta delle prove informatiche non è stata conforme al modello legale, la circostanza riverbererà i suoi effetti sul valore e sull'intensità della prova medesima, che sarà nondimeno utilizzabile ai fini della decisione, ma poco attendibile e dunque inidonea da sola a fondare un giudizio di colpevolezza secondo il prudente apprezzamento del giudice"[150].

Altra dottrina riconosce la nullità delle prove informatiche raccolte in violazione delle misure tecniche idonee a preservarne la genuinità. "Se dunque non fossero attuate le misure di conservazione e salvaguardia dei dati originali, l'ispezione o la perquisizione sarebbero nulle; di conseguenza anche le prove raccolte (si pensi ad esempio ad un *file* di *log*) sarebbero anch'esse nulle"[151].

Occorre ricordare, inoltre, che la l. n. 48 del 2008 con i suoi numerosi interventi codicistici, di fatto implicitamente riconosce una inammissibilità probatoria, ribadendo il ricorso alla regola della "estromissione dal processo d'ogni materiale inquinato capace di adulterare la ricostruzione penale"[152].

[150] G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in Luparia L. (a cura di), "Sistema penale e criminalità informatica", Milano, Giuffrè, 2009, p. 190 e ss. Sull'argomento cfr. la posizione della giurisprudenza che ritiene sia da invocare una inutilizzabilità della prova solo nei casi di violazione di divieti espressi, cfr. Cass. Pen., I, 23 marzo 1994, in "Giustizia penale", 1996, III, p. 363 e ss.; Cass. Pen., sez. I, 12 gennaio 2011, n. 5095, in CED Cass. pen., 2011.

[151] E. VITALE, *La ratifica della Convenzione del Consiglio d'Europa sul cybercrime. La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in "Diritto dell'Internet", 2008, n. 5, p. 509 e ss.

[152] Specificamente sull'argomento L. LUPARIA, *Computer crimes e procedimento penale*, cit.,

La rogatoria è strettamente connessa alla fase della raccolta delle prove rivelandosi necessaria qualora l'autorità giudiziaria, nel corso di un processo "pendente presso di sé", debba eseguire atti processuali in luoghi fuori della propria competenza territoriale o giurisdizione. Brevemente si ricorda che la rogatoria può essere nazionale (c.d. rogatoria interna) oppure straniera (c.d. rogatoria internazionale).

Nel caso "Melania Rea" si è parlato di una rogatoria internazionale penale. Questo tipo di rogatorie nel nostro ordinamento giuridico sono disciplinate dagli artt. 723-729 c.p.p.[153]. Specificamente gli artt. 723-726 *ter* c.p.p. disciplinano le c.dd. rogatorie passive (ossia che provengono dall'estero) mentre gli artt. 727-729 c.p.p. regolano le rogatorie attive (ossia quelle che è la nostra autorità giudiziaria ad inoltrare all'estero). Oltre al codice di procedura penale regolano la materia anche norme internazionali come la Convenzione europea di assistenza giudiziaria firmata a Strasburgo il 20 aprile 1959[154]. Dietro alla disciplina normativa vi è una procedura burocratica piuttosto articolata che vede coinvolte sia le autorità diplomatiche sia quelle politiche[155].

12. Prova e riferimenti normativi

"Dobbiamo imparare bene le regole per infrangerle nel modo giusto"
Dalai Lama

Nel 1995 una interessante *Recommendation No. R (95) 13 Council of Europe Comittee of Ministers*[156], relativa ai problemi di procedura penale legati

p. 389.

[153] Libro XI Rapporti giurisdizionali con autorità straniere.

[154] Aggiornata dall'Accordo italo-svizzero del 10 settembre 1998 che è stato ratificato in Italia dalla l. 5 ottobre 2001, n. 367 la quale ha di fatto modificato i citati articoli del codice di procedura penale (specificamente ha introdotto l'art. 729 c.p.p).

[155] L'autorità diplomatica come canale di trasmissione mentre il Ministro della giustizia con funzione "propulsiva". L'autorità giudiziaria, da parte sua, può agire "autonomamente" sia nell'ipotesi di rogatoria passiva bloccandola (qualora sussistano circostanze impeditive) sia nell'ipotesi di rogatoria attiva, inoltrandola "direttamente" ed informando di ciò il Ministro successivamente, qualora questi non si sia attivato entro il tempo richiesto o in caso di urgenza. Per approfondimenti sul tema si rinvia a studi di settore.

[156] http://www.coe.int/t/dghl/standardsetting/media/doc/cm_EN.asp oppure in Problems of criminal procedural law connected with information technology: recommendation No. R (95) 13 adopted by the Committee of Ministers of the Council of Europe on 11 September 1995, and explanatory memorandum, Council of Europe, 1996.

alla tecnologia dell'informazione, indicava ai Governi degli Stati membri

- "di ispirarsi, nel momento in cui modificano le rispettive legislazioni e procedure interne, ai princìpi che si trovano in annesso a questa Raccomandazione;
- di fare conoscere queste disposizioni alle autorità incaricate delle inchieste e agli altri uffici professionali, in particolare, al settore della tecnologia dell'informazione, che possano essere interessati alla problematica per il tipo di attività svolta".

Altre indicazioni riguardavano gli aspetti legati alla perquisizione ed al sequestro; gli obblighi di cooperazione con le autorità incaricate dell'inchiesta e la *digital evidence* (la prova elettronica, "L'interesse comune di raccogliere, di salvaguardare e di esibire prove elettroniche in modo da garantire al meglio il carattere inconfutabile e l'integrità di esse dovrebbe essere riconosciuto sia per avviare azioni giudiziarie nazionali che per svolgere attività di cooperazione internazionale. A tale fine, procedure e metodi tecnici per il trattamento delle prove elettroniche dovrebbero essere sviluppati preventivamente in modo da assicurarne la compatibilità tra Stati. Le disposizioni del diritto di procedura penale concernenti le prove e riferibili a documenti tradizionali dovrebbero ugualmente applicarsi ai dati immagazzinati in un sistema informatico").

Il principale riferimento normativo alla base dello scenario investigativo e processuale analizzato è rappresentato dalla l. n. 48/2008 che recepisce la Convenzione di Budapest sul *cyber crime*[157].

La Convenzione di Budapest del 23 novembre 2001[158], emanata dal Consiglio europeo in tema di criminalità informatica, è, in realtà, il primo accordo internazionale sui crimini commessi attraverso Internet o altre reti informatiche. Il suo intento è di permettere una collaborazione ed una legislazione coordinate fra gli Stati membri in grado di affrontare in maniera incisiva la criminalità informatica.

[157] Sul testo normativo cfr. L. PICOTTI, *Ratifica della convenzione cybercrimine e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in "Diritto dell'Internet", 2008, p. 437 e ss. e G. Ilarda, G. Marullo (a cura di), *Cybercrimine. Conferenza internazionale. La Convenzione del Consiglio d'Europa sulla criminalità informatica*, Milano, Giuffrè, 2004, *passim*.

[158] Alla redazione della Convenzione hanno contribuito ben 144 Paesi, tra i quali anche Canada, Stati Uniti e Giappone. Il testo è consultabile all'indirizzo www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Per approfondimenti si consiglia la consultazione del Dossier contenuto nello stesso sito.

Nella Convenzione di Budapest sono previsti, inoltre, meccanismi di cooperazione internazionale, a livello europeo, con riferimento sia ad istituti tradizionali, quali l'estradizione e la rogatoria (*ex* artt. 24, 25 e 26 Convenzione) sia ad ipotesi nuove di collaborazione, tra le quali: la conservazione dello stoccaggio dei dati e la rapida divulgazione delle informazioni inerenti il traffico degli stessi (*ex* artt. 29, 30, 32 e 35 Convenzione).

La norma di recepimento del 2008 delinea sostanzialmente gli aspetti inerenti la cooperazione internazionale; la competenza nello svolgimento delle indagini e nell'esercizio dell'azione penale; i fornitori di servizi; il fenomeno della *data retention*; il sequestro di corrispondenza e il conseguente sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazione[159]. Ma ciò che viene messo in evidenza ed espressamente riconosciuto dal nostro legislatore, con la l. n. 48 del 2008, è il peso determinante delle procedure e delle tecniche di *computer forensic*, attraverso la predisposizione di procedure volte ad assicurare una corretta acquisizione, conservazione, inalterabilità ed immodificabilità della prova informatica.

Un breve cenno merita il d.lgs. n. 231 del 2001 che ha introdotto nel nostro ordinamento la figura della responsabilità amministrativa degli enti, qualora questi commettano o tentino di commettere specifici reati (espressamente previsti nella norma) per il proprio interesse o per il proprio vantaggio (art. 5, co. 1). Fra i reati previsti nella norma ci sono i delitti informatici ed il trattamento illecito di dati *ex* art. 24 *bis* a sua volta introdotto dall'art. 7 della pluricitata e onnipresente l. n. 48 del 2008, che in tal modo ha ampliato i "reati" in grado di generare la responsabilità in capo alla società.

La commissione dei reati deve essere effettuata dalle persone che sono al vertice dell'ente e/o da coloro che a questi sono sottoposti.

Il decreto legislativo penalizza direttamente l'ente attraverso l'applicazione di sanzioni pecuniarie, l'interdizione dall'attività, l'eventuale commis-

[159] Qui scatta la previsione delle procedure inerenti alla raccolta delle prove che permette all'autorità giudiziaria di stabilire, laddove sussistano delle esigenze per la regolare fornitura dei servizi, le modalità di acquisizione dei dati sottoposti a sequestro così che possa avvenire "mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità" *ex* art. 254 *bis* c.p.p. (con indiretto e conseguente obbligo del fornitore di "conservare e proteggere adeguatamente i dati originali"). Interessante il contributo di S. MONTELEONE, *Alcune riflessioni sull'impiego della prova elettronica in giudizio*, in http://www.teutas.it/societa-informazione/prova-elettronica/264-alcune-riflessioni-sullimpiego-della-prova-elettronica-in-giudizio.html e che (si cita l'autore) "trae spunto principalmente dai risultati del progetto europeo The Admissibility of Electronic Evidence before Courts.

sariamento o il divieto a contrarre con la Pubblica Amministrazione. Sostanzialmente colpisce direttamente il patrimonio dell'ente "colpevole" ed indirettamente l'interesse economico dei soci.

L'ente non è responsabile qualora dimostri di avere adottato un documento (Modello) contenente indicazioni da seguire al fine di evitare il verificarsi dei reati previsti[160] e qualora provi che i soggetti che hanno commesso il reato lo abbiano fatto fraudolentemente eludendo i modelli di organizzazione e di gestione di cui sopra (art. 6, lett. *c*).

Altro testo di riferimento è la citata direttiva n. 24 del 2006 recepita dal d.lgs. 30 maggio 2008, n. 109 sul *data retention* ed inerente il delicato rapporto tra controllo della sicurezza e rispetto della *privacy* degli utenti/cittadini.

In precedenza il legislatore nazionale aveva emanato la l. 23 dicembre 1993, n. 547, recante modifiche al codice penale e di procedura penale[161].

Altra norma da ricordare è la l. 3 agosto 1998, n. 269 contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù; con estensione a fenomeni di pedopornografia virtuale (l. 6 febbraio 2006, n. 38).

Ulteriori interventi legislativi si sono concentrati su aspetti che potrebbero essere definiti marginali ma che hanno, comunque, un ruolo nel regolamentare le attività in ambiente digitale, così ad esempio la l. 8 agosto 2000, n. 248 in materia di tutela del diritto di autore e pirateria informatica, op-

[160] Per ulteriori approfondimenti si rinvia alla produzione dottrinale di settore. In questo contesto cfr., per tutti, G. LATTANZI (a cura di), *Reati e responsabilità degli enti. Guida al d.lgs. 8 giugno 2001*, n. 23, Milano, Giuffrè, 2010, *passim*; P. PREVITALI, *Modelli organizzativi e compliance aziendale. L'applicazione del d.lgs. 231/2001 nelle imprese italiane*, Milano, Giuffrè, 2009, *passim*.

[161] La norma, di fatto, ha introdotto "nuovi" reati integrando o inserendo gli articoli del codice penale: "Esercizio arbitrario delle proprie ragioni con violenza sulle cose" (art. 392, co. 3, c.p.); "Attentato ad impianti di pubblica utilità" (art. 420 c.p); "Accesso abusivo ad un sistema informatico o telematico" (art. 615 *ter* c.p.); "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici" (art. 615 *quater* c.p.); "Diffusione di programmi diretta a danneggiare o interrompere un sistema informatico" (art. 615 *quinquies* c.p.); "Danneggiamento di sistemi informatici o telematici" (art. 635 *bis* c.p.); "Frode informatica" (art. 640 *ter* c.p.); "Violazione, sottrazione e soppressione di corrispondenza" (art. 616 c.p.); "Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche" (art. 617 *quater* c.p.); "Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche" (art. 617 *quinquies* c.p.); "Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche" (art. 617 *sexies* c.p.); "Falsità informatica" (art. 491 *bis* c.p.); "Altre comunicazioni e conversazioni" (art. 623 *bis* c.p.).

pure il d.l. n. 143 del 1991, art. 12, convertito in l. 5 luglio 1991, n. 197, che detta provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio.

Relativamente alla *privacy* si è già citato il d.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

Per finire, occorre ricordare la l. 31 luglio 2005, n. 155, recante "Misure urgenti per il contrasto del terrorismo internazionale" che all'art. 7 *bis* attribuisce, di fatto, al Servizio Polizia Postale e delle Comunicazioni, in via esclusiva ed in virtù delle proprie specialistiche competenze, la protezione dei sistemi informatici delle infrastrutture critiche di interesse nazionale[162].

Gli interventi del legislatore si sono sviluppati anche nei vari Codici di settore.

Nel codice civile e nel codice di procedura civile i principali articoli di riferimento sono il 2702 ed il 2712 (quest'ultimo prevede anche le riproduzioni informatiche equiparandole alle rappresentazioni meccaniche di fatti e di cose che formano piena prova dei fatti e delle cose rappresentate) letti in combinato disposto con gli artt. 214, sul disconoscimento della scrittura privata, e 215, sul riconoscimento tacito della scrittura privata, c.p.c.

Il codice di procedura penale è, indubbiamente, il testo di riferimento normativo più rilevante in grado di regolare lo scenario investigativo digitale, soprattutto dopo i numerosi interventi della l. n. 48 del 2008. Fra gli articoli del codice che trattano dello specifico argomento si ricordano:

- l'art. 51 inerente gli uffici del p.m. e le attribuzioni del procuratore della Repubblica, spec. al co. 3 *quinquies*;
- l'art. 55 in merito alle funzioni della polizia giudiziaria;
- l'art. 234 sulla prova documentale e definita come una sorta di "norma aperta"[163];
- l'art. 244 con riferimento ai casi ed alle forme di ispezione;
- l'art. 247 (e il correlato art. 248) relativo all'istituto della perquisizione e che con l'art. 8, co. 2, della l. n. 48 del 2008, si è arricchito di un ulteriore comma, 1 *bis*, che così recita "Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informa-

[162] Cfr. Circolare del 29 agosto 2005 in http://www.interno.it.

[163] Nel co. 2 dell'art. si legge, inoltre, che esiste la possibilità di utilizzare anche la copia della prova (documento) qualora questo sia stato distrutto o si sia smarrito, potendo rientrare nell'ipotesi di legge anche la esibizione degli stampati di documenti elettronici.

tico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione";
- l'art. 253 che tratta dell'oggetto e delle formalità legate al sequestro ed il conseguente art. 254, sul sequestro di corrispondenza;
- l'art. 254 *bis* sempre prodotto dalla l. n. 48 del 2008, inerente il sequestro di dati informatici presso i fornitori di servizi informatici, telematici e di telecomunicazioni;
- l'art. 260 in riferimento alla fase dell'apposizione dei sigilli alle cose sequestrate;
- l'art. 266 *bis*, tra i primi interventi del nostro legislatore sui reati "commessi mediante l'impiego di tecnologie informatiche e telematiche";
- l'art. 348 sull'assicurazione delle fonti di prova;
- l'art. 352 in tema di perquisizioni e flagranza di reato soprattutto in seguito alla modifica della l. n. 48 del 2008 che con l'art. 9 ha aggiunto al "vecchio" testo il co. 1 *bis* affinché sia assicurato l'intervento della p.g. attraverso la "(...) perquisizione di sistemi informatici o telematici, ancorchè protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi";
- l'art. 354 per quanto riguarda lo specifico ambito della ricerca delle fonti di prova e che al co. 2 così recita: "Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti"[164];

[164] C.d. procedura di duplicazione rispettosa della conformità della copia all'originale e

- l'art. 359 in merito alla nomina di consulenti tecnici;
- l'art. 360 sugli accertamenti tecnici irripetibili, articolo che offre alla persona indagata la facoltà di nominare consulenti tecnici[165]. In merito alle attività del perito e dei c.dd. consulenti tecnici si rinvia anche agli artt. 228 e 230.

Per ultime si citano le norme che regolano la corretta esibizione delle prove nelle varie fasi del processo, necessarie per permetterne una giusta valutazione da parte del giudice e determinare, quindi, la "formazione del convincimento". Così ad esempio gli artt. 187, 189 (particolarmente interessante ai fini delle prove non espressamente disciplinate dalla legge eppure idonee ad essere valutate tali dal giudice), 190, 190 *bis* e 191 c.p.p.

Il "Codice dell'amministrazione digitale" - CAD è, anch'esso attento ad uniformare il nostro Paese alle indicazioni normative europee[166], anche nella parte in cui regola la creazione e l'efficacia probatoria del documento informatico (art. 21 CAD), della sua formazione, ossia del rispetto delle regole e delle indicazioni contenute nel testo normativo, ai fini del riconoscimento della sua efficacia probatoria (*ex* art. 71 CAD). Il Codice prevede anche l'efficacia probatoria della Pec (artt. 45 e 48 CAD), rinviando e ricollegandosi anche agli articoli del codice civile sulle prove (2702 e 2712 c.c.). Sono previsti, inoltre, inasprimenti della pena qualora i reati vengano commessi da particolari soggetti, come ad esempio gli amministratori di sistema, che a causa della loro funzione hanno la possibilità di accedere ad aree riservate dei sistemi informativi. In sostanza viene ribadita una circostanza aggravante, per approfittamento, già prevista nell'art. 61, n. 11, c.p.

13. Prova e documento informatico

"Datemi sei righe scritte dal più onesto tra gli uomini
e vi troverò materiale sufficiente a farlo impiccare"

della sua immodificabilità.

[165] In tema di attività di consulenza e del coinvolgimento di periti o di tecnici di parte, si ricorda brevemente che il *sopralluogo* è considerato un mezzo di ricerca della prova perché rende possibile l'acquisizione di cose o il rilevamento di tracce dotate di attitudine. Questa ricerca della prova consiste in un vero e proprio atto ispettivo volto a descrivere e riprodurre la scena del crimine nel modo più fedele ed incontaminato possibile. La perizia tenta di dare un vero e proprio giudizio tecnico e comunque una valutazione che siano il più possibile precisi e coerenti con l'evento analizzato, così da poter fornire una risposta chiara ai quesiti posti dal magistrato. Il legame tra le due fasi sta nel fatto che la perizia si basa (o comunque non può ignorare) a sua volta sugli elementi oggettivi raccolti durante il sopralluogo.

[166] Cfr. in proposito la direttiva n. 99/93/CE sullo sviluppo dell'*e-government*.

Richelieu

Quando si parla di prova informatica è naturale accennare al documento informatico ed al suo valore probatorio.

Come già accennato, nel CAD si occupano del documento informatico e delle relative firme elettroniche gli artt. 20, co. 2, e 21, con espresso riferimento all'art. 2702 c.c.

Nell'art. 20, co. 1, si afferma che "Il documento informatico da chiunque formato, la *memorizzazione* su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'art. 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice" e che "L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità" (co. 1 *bis*).

Nell'art. 21 viene fatta una duplice affermazione: la prima consiste nel fatto che il documento informatico con firma elettronica (debole/semplice) ha una efficacia probatoria rilasciata alla libera valutazione del giudice il quale "gradua" la capacità probatoria in ragione delle sue caratteristiche tecniche; la seconda, che il documento informatico sottoscritto da una firma digitale ha piena efficacia probatoria a meno che non venga fatta valere nei suoi confronti una querela di falso, non sia, cioè, disconosciuto dal soggetto che lo ha sottoscritto e contro il quale viene esibito.

Si intende per "scrittura privata" il documento che viene redatto per iscritto, con qualunque mezzo, sia esso cartaceo o elettronico, e sottoscritto dall'autore della dichiarazione. Può, dunque, essere redatta sia su carta sia in versione informatica e, se sottoscritta, ha natura di prova precostituita. Quando nell'articolo si fa riferimento a "piena prova" si vuol intendere che quel documento (dichiarazione) se sottoscritto (scrittura privata) è la prova della dichiarazione della volontà del soggetto che l'ha firmato.

L'art. 23 del CAD tratta delle copie del documento informatico, affermando che "Le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato". Inoltre stabilisce che "Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro confor-

mità non è espressamente disconosciuta. Resta fermo, ove previsto l'obbligo di conservazione dell'originale informatico".

L'art. 23 *quater* in tema di riproduzioni informatiche dispone l'aggiunta del termine "informatiche" al testo dell'art. 2712 c.c. riconoscendo al documento informatico l'efficacia probatoria delle riproduzioni "meccaniche" che fanno piena prova dei fatti in esso rappresentati.

Il codice penale nell'art. 491 *bis*, trattando dei documenti informatici, afferma che "Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private". La norma è stata collocata nel Libro II del codice penale che tratta della violazione di fede pubblica documentale. Sembrerebbe, dunque, che il legislatore nella "Impossibilità di ricondurre il controllo penale delle manipolazioni informatiche nell'area della tradizionale nozione di documento ha imposto, dunque, l'introduzione nel codice penale della disposizione di cui all'art. 491 *bis* c.p., che prevede una sostanziale equiparazione, ai soli fini delle disposizioni sulle falsità in atti contenuti nel codice penale, del documento informatico agli atti pubblici ed alle scritture private"[167].

[167] G. DE AMICIS, in Lattanzi G., Lupo E., "Codice penale. Rassegna di giurisprudenza e di dottrina", Vol. 10, in Ciani G., Conforti A., De Amicis G., Ebner G., Gambardella M., Lattanzi C., Napoleone V., Silvestri P. (a cura di), "I delitti contro la fede pubblica, i delitti contro l'economia pubblica, l'industria e il commercio, i delitti contro la moralità pubblica e il buon costume e i delitti contro il sentimento per gli animali, Libro II, artt. 453-555", Milano, Giuffrè, 2010, p. 652. Cfr. anche R. BORRUSO, G. BUONOMO, G, CORASANITI, G. D'AIETTI, *Profili penali dell'informatica*, Milano, Giuffrè, 1994, p. 16. Sul documento informatico e su tutte le problematiche connesse sia alla sua efficacia probatoria sia alla regolamentazione in materia da parte del CAD si rinvia alla copiosa letteratura prodotta. Cfr. per tutti: A. GENTILI, *I documenti informatici: validità ed efficacia probatoria*, in "Diritto dell'Internet", 2006, n. 3, p. 297; U. SILVESTRONI, *Spunti sul vecchio e nuovo formalismo*, in "Rivista trimestrale di diritto e procedura civile", 2006, n. 2, p. 421; P. CORSINI, E. ORBINI MICHELUCCI, *Sostituire il documento cartaceo con il documento informatico, firmarlo e trasmetterlo via rete*, in "Diritto dell'Internet", 2006, n. 3, p. 311; A. GRAZIOSI, *La nuova efficacia probatoria del documento informatico*, in "Rivista di diritto e procedura civile", 2003, n. 1, p. 53 e ss. V. inoltre le monografie di R. BORRUSO, G. CIACCI, *Diritto civile e informatica*, Napoli, ESI, 2005; M. CAMMARATA, *Firme elettroniche, problemi normativi del documento informatico*, Pescara, Monti e Ambrosini Editori, 2007; L. PICOTTI, *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, Cedam, 2011 e C. SARZANA DI SANT'IPPOLITO, *Informatica, Internet e diritto penale*, Milano, Giuffrè, 2010.

14. RESPONSABILITÀ

Gli ISP - Internet Service Providers sono spesso, loro malgrado, automaticamente coinvolti nei crimini che vedono l'uso di strumenti informatici e per questo motivo il legislatore ha da sempre avvertito la necessità di prevedere una serie di interventi normativi contenenti obblighi specifici legati al loro ruolo. Ad esempio, nell'ipotesi di pedopornografia, esiste l'obbligo di utilizzo di strumenti di filtraggio (come ad esempio la compilazione e l'aggiornamento di vere e proprie *black list*) di indirizzi Internet di natura pedopornografica e di adozione di "relative soluzioni tecnologiche" (come ad esempio approntare sistemi informatici *ad hoc*) in grado di impedire l'accesso o comunque la consultazione di siti che diffondono materiale pedopornografico (*ex* art. 14 *quater* della l. 3 agosto 1998, n. 269, così come introdotto dall'art. 19 della l. n. 38 del 2006).

Sostanzialmente gli ISP debbono collaborare con il *law enforcement* poiché appaiono i soggetti più idonei a rilevare i contenuti illeciti presenti in Rete. La ratifica della Convenzione sul *cyber crime* ha condizionato fortemente il *service provider* a obblighi di collaborazione, consegna e conservazione prolungata dei dati.

Gli artt. 14, 15, 16, nonché 17, del d.lgs. n. 70 del 2003 (sul commercio elettronico) contengono questi obblighi in violazione dei quali scatterebbe la responsabilità dei *provfider* e dei prestatori di servizi in genere. Il condizionale è d'obbligo, perché la caratteristica del testo di legge consiste in una sorta di decalogo di responsabilità al negativo, dove la responsabilità viene dedotta "per esclusione" in quanto negli articoli indicati il legislatore prevede tutti quei casi in cui il prestatore "non" risulta responsabile.

Nell'analisi degli articoli si deduce la definizione di *provider* e la sua responsabilità.

Il *provider* può essere un prestatore intermediario, qualora la sua attività imprenditoriale consista nell'offrire servizi di connessione trasmissione ed immagazzinamento dei dati o nel permettere che un sito di altri possa risiedere ed essere gestito dalle proprie apparecchiature.

L'art. 14 tratta della "Responsabilità nell'attività di semplice trasporto" e recita: "1. Nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione, il prestatore non è responsabile delle informazioni trasmesse a condizione che: a) non dia origine alla trasmissione; b) non selezioni il

destinatario della trasmissione; c) non selezioni né modifichi le informazioni trasmesse. 2. Le attività di trasmissione e di fornitura di accesso di cui al comma 1 includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo. 3. L'autorità giudiziaria o quella amministrativa, avente funzioni di vigilanza, può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 2, impedisca o ponga fine alle violazioni commesse". Nell'articolo viene data la definizione di attività di *mere conduit*, ossia di semplice trasmissione di informazioni o di semplice fornitura di accesso alla rete. In questa ipotesi non è configurata alcuna responsabilità del prestatore, a meno che egli stesso non partecipi alla produzione o alla modifica delle informazioni oppure selezioni il destinatario della trasmissione.

L'art. 15 si occupa della responsabilità nell'attività di memorizzazione temporanea, nota come *caching* e recita: "1. Nella prestazione di un servizio della società dell'informazione, consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che: a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione. 2. L'autorità giudiziaria o quella amministrativa aventi funzioni di vigilanza può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse". Anche qui viene data, prima, la definizione di attività di *caching*, che consiste nella memorizzazione temporanea o transitoria delle informazioni trasmesse, e successivamente viene affermata la non-responsabilità del prestatore a meno

che egli non intervenga direttamente sulle informazioni ospitate nelle sue strutture informatiche.

L'art. 16 parla dell'attività di *hosting*, cioè dell'attività di memorizzazione duratura e stabile delle informazioni immesse in rete dai propri clienti ed anche qui viene ribadita la non-responsabilità dell'operatore qualora: a) il soggetto non sia a conoscenza del loro contenuto illecito; b) ed una volta a conoscenza non interviene prontamente per rimuoverle.

L'art. 17 contiene l'affermazione di un principio di assenza dell'obbligo generale di sorveglianza in capo al prestatore di servizi: "1. Nella prestazione dei servizi di cui agli artt. 14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite". Indirettamente la norma esclude la possibilità di inquadrare la responsabilità in esame secondo il criterio dell'oggettività (*ex* artt. 2050, Responsabilità per l'esercizio di attività pericolose e 2051, Danno cagionato da cosa in custodia, c.c.) adeguandosi all'atteggiamento del legislatore comunitario che non sembra voler attribuire al prestatore una responsabilità oggettiva legata al tipo di attività svolta, preferendo ipotizzare quella articolata e poco chiara responsabilità "al negativo" di cui si è accennato.

Nel co. 2 dell'art. 17 è prevista una forma che mitiga il pericolo di una eccessiva "deresponsabilizzazione" del soggetto, e cioè la cooperazione nell'attività di prevenzione degli illeciti sulla rete, cooperazione che, peraltro, sembra superfluo ribadire in quanto dovuta per legge: "2. Fatte salve le disposizioni di cui agli artt. 14, 5 16, il prestatore è comunque tenuto: a) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; b) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite." Nell'ipotesi in cui non si ottemperi a questi obblighi potrebbe essere invocato l' art. 378 c.p. che prevede l'ipotesi di favoreggiamento personale, in caso di reato, ferma restando la responsabilità civile ribadita nel co. 3, laddove: "(...) richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo

del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente".

A livello concreto i *provider* possono essere chiamati ad esibire, dietro richiesta dell'autorità, i c.dd. *log file* che di fatto mantengono traccia delle attività svolte dagli utenti durante le loro navigazioni in rete. Questi preziosi elementi informatici, pur non essendo dati personali veri e propri contengono, in realtà, informazioni equiparabili (ormai abbastanza unanimemente[168]) a dati sensibili e, perciò, adeguatamente protetti.

15. File di log

Quando si parla di *log file* è opportuno ricordare la loro origine prettamente informatica, volta a determinare i carichi di lavoro dei *server* e studiare possibili migliorie nella loro distribuzione. Con il passare del tempo ci si è accorti che i dati in essi contenuti permettono di monitorare il traffico dei visitatori della rete. Questa loro potenzialità ha spinto il legislatore a regolamentarne la raccolta per gestire in modo lecito questa nuova forma di dati.

Le informazioni presenti nei *log*, se opportunamente confrontate, sono in grado sia di controllare l'utente che li ha generati (come nell'ipotesi del lavoratore che utilizza gli strumenti informatici dell'azienda) sia di profilare l'ignaro navigatore per scopi di *business*.

Un loro corretto utilizzo presenta rilevanti vantaggi come, ad esempio, testare il funzionamento ed il gradimento di un sito *web*, fidelizzare il cliente/utente offrendo prodotti o servizi in base alle sue preferenze, agevolare, in genere, la navigazione dell'utente.

Le regole per un lecito trattamento dei *file* di *log* sono contenute nel "Codice della privacy", con particolare riferimento al già citato art. 132 che, nonostante la sua specifica portata, resta inquadrato nell'ambito delle regole generali per il trattamento dei dati (Titolo III). Si ricorda, inoltre, il rinvio al principio di proporzionalità ossia al divieto di raccolta dati qualora questa risulti superflua o inutile e comunque non pertinente perché eccessiva ai fini

[168] Lo stesso Garante della privacy prevede il trattamento di *file* di *log* "in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai *file* di *log* riferiti al traffico *web*, su base collettiva o per gruppi sufficientemente ampi di lavoratori)" cfr. Deliberazione 1 marzo 2007 in http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522.

del conseguimento dello scopo prefigurato[169].

Anche il d.lgs. n. 70 del 2003 prevede alcuni articoli indirettamente riferibili al trattamento dei *log file* in quanto dedicati alla tutela del consumatore.

I *file* di *log* telematici vengono acquisiti con decreto motivato del Pubblico Ministero, anche su richiesta del difensore dell'imputato, ma anche della persona sottoposta alle indagini, della persona offesa e delle altre parti private[170]. Il decreto va notificato o al *provider* o alla società che gestisce la risorsa sotto indagine così da poter ottenere le informazioni desiderate sull'utente e sul CLI (*Calling Line Identifier*, ossia l'dentificativo del chiamante) utilizzato per connettersi.

Nel 2005 la giurisprudenza penale, si è espressa sui *file* di *log* con una interessante sentenza della Cassazione[171]. Nella decisione viene affermata la punibilità, *ex* art. 600 *quater*, del possesso di materiale pornografico avvenuto attraverso il salvataggio su pc o altri supporti, escludendo l'illiceità della mera consultazione (semplice navigazione e monitoraggio) dei siti *web* di contenuto pornografico, navigazione provata attraverso l'acquisizione dei *file* di *log*. Viene confermato, così, un precedente orientamento[172] in merito alla registrazione dei *file* temporanei che non proverebbero l'elemento soggettivo "dell'illecita disposizione/detenzione in quanto di difficile percezione da parte degli utenti"[173].

16. CASI DI STUDIO

"Utrumque enim vitium est, et omnibus credere, et nulli"
Seneca

Stato del Connecticut contro Julie Amero. Il primo caso è noto come "Julie Amero"[174]. Verificatosi nel 2004 è stato giudicato per la prima volta nel

[169] I parametri sono pochi e chiari: informativa nei confronti dell'utente; preventivo consenso; impegno a non cedere a terzi i dati raccolti senza una apposita autorizzazione dell'interessato. Sul trattamento dei *file* di *log* e sui loro profili giuridici cfr. anche A. GHIRARDINI, G. FAGGIOLI, *Computer forensics*, Piacenza, Apogeo, 2007, p. 37, spec. p. 40.

[170] Art. 132, co. 3, d.lgs. n. 196 del 2003.

[171] Cass. Pen., sez. III, 21 settembre 2005, n. 39282, in Cassazione penale, n. 9, 2005 e in http://www.penale.it/page.asp?mode=1&IDPag=106..

[172] Tribunale di Perugia, 8 luglio 2003, n. 313 (dep. 30 dicembre 2003) in http://www.penale.it.

[173] Sulla conservazione dei dati informatici nell'ambito delle indagini informatiche cfr. F. CAJANI, *Alla ricerca del log (perduto)*, in "Diritto dell'Internet", 2006, n. 6, p. 572 e ss.

[174] Superior Court New London Judicial District at Norwich, GA 21; 3, 4 and 5 January

2007 e chiuso nel 2008[175]. È un caso classico che dimostra quanto possa essere complesso il repertamento di prove informatiche. Il fatto si è verificato in una scuola di Norwich nel Connecticut (*Kelly Middle School*) ed ha coinvolto una insegnante che per la sua scarsa conoscenza degli strumenti informatici ha rischiato 40 anni di reclusione per aver mostrato del materiale porno agli alunni in classe. Questi, infatti, hanno visionato una "prorompente cascata" di *pop-up* dal contenuto esplicitamente erotico e pornografico. L'accusa mossa nei confronti dell'insegnante era di aver "volontariamente" proposto questo materiale ai minori. Si è giocato molto sul termine "volontariamente" in quanto l'insegnante, poco pratica di pc, non è riuscita, in realtà, ad interrompere il susseguirsi di materiale che compariva sulla videata. Come affermato dalla difesa che ha chiamato un perito di parte a testimoniare, il computer era letteralmente infestato da *spyware* richiamati da un sito di acconciature alla moda che avrebbe favorito l'accesso al pc della scuola agganciandosi alla vulnerabilità del *browser*.

In realtà la difesa, pur avendo avuta la possibilità di contrattaccare, replicando (e soprattutto dimostrando) che lo *spyware* era presente nel computer della scuola già prima che venisse utilizzato dalla Amero[176], non era riuscita, nel primo processo, ad approntare una condotta difensiva adeguatamente valida anche e soprattutto a causa della complessità delle perizie tecniche che il caso richiedeva. Durante il processo venne fatto notare che la polizia aveva visionato l'hard disk senza tuttavia farne una copia in *bit-stream*. Successivamente un magistrato ha chiesto ed ottenuto l'annullamento della condanna dell'insegnante, promuovendo un nuovo processo nel quale Julie Amero è stata giudicata in base alla testimonianza ed alle analisi delle prove digitali esibite da periti informatici. Finalmente nel 2008 si è giunti alla chiusura del caso e l'unica colpa riconosciuta all'insegnante è stata quella di non aver "reagito con prontezza" spegnendo brutalmente il computer.

Per la serie "prevenire è sempre meglio che curare" il caso Julie Amero ha dato, in seguito, l'*input* per la costituzione (negli USA) di una serie di associazioni in grado di fornire apposite istruzioni così da poter verificare se

2007 (Docket number CR-04-93292); cfr., inoltre, per ulteriori informazioni, il sito inglese http://en.wikipedia.org/wiki/State_of_Connecticut_v._Julie_Amero.

[175] Sembra con un patteggiamento in cui è decaduta l'imputazione di rischio di lesioni a minore dietro l'assunzione da parte dell'insegnante di un riprovevole atteggiamento di "condotta disordinata".

[176] Spostando così la responsabilità verso lo stesso Istituto, "colpevole" di possedere e far utilizzare ad insegnanti e studenti, computer poco sicuri.

il proprio pc sia diventato uno "zombie computer"[177] oppure no.

Il *caso Garlasco*. Il caso in esame è l'espressione classica di "alibi informatico". Nel 2007 Alberto Stasi viene indagato per l'omicidio della sua fidanzata Chiara Poggi. Viene assolto[178] da questa accusa grazie al suo "alibi informatico". Stasi, infatti, afferma che il 13 agosto del 2007, giorno dell'omicidio, non era sul luogo del delitto in quanto dopo essersi svegliato alle ore 9, ed aver telefonato alla sua ragazza, aveva iniziato a lavorare alla propria tesi sul suo pc. A dimostrazione di queste affermazioni mette a disposizione dei carabinieri il proprio computer. Tuttavia, prima che ne venga effettuata una copia forense, il pc è oggetto di ripetuti accessi scorretti, effettuati da investigatori non esperti in violazione delle tecniche forensi di indagine. Vengono così violate le disposizioni del codice di procedura penale con conseguente pericolo di inficiare il valore probatorio del procedimento di acquisizione della prova.

La difesa dell'imputato eccepiva, così, l'inutilizzabilità, come fonte di prova, del contenuto del computer portatile di Stasi.

Nonostante gli effetti devastanti delle maldestre operazioni compiute sul pc, il collegio peritale è riuscito, tuttavia, ad ottenere egualmente particolari informazioni fuori dal sistema operativo (attraverso i c.dd. metadati) raggiungendo l'intento di provare la certezza dell'interazione "diretta e sostanzialmente continuativa dell'utente con il computer". In base a questa perizia (ed evidentemente ad altre prove) il giudice (dr. Vitelli) assolse Stasi dall'accusa di omicidio.

Resta in sospeso, la inquietante scoperta di alcuni *file* che sono stati scaricati dalla vittima su di una chiavetta USB in merito ad alcuni articoli di *cold*

[177] Così P. GUERRERA, *Attenzione a worm e virus: il caso Julie Amero ha fatto scuola*, in http://www.pcworld.it/ del 2007. Alcuni volontari del c.d. Julie Project informano attraverso un Blog (http://thejuliegroup.blogspot.com/) dove viene ribadito che "Readers are expected to think about the issues, question everything worth discussing, and add value to the conversation by correcting what's here or broadening the understanding of the subject. This is part of the educational process between us all. Our hope is that this exercise results in better law, law enforcement, and citizen participation in forging sophisticated social understandings of the technological forces changing our lives" e una Wiki page (http://thejuliegroup.pbworks.com) dove si legge "Our Purpose: To bring attention to those situations where injustice is being done through the misuse or misunderstanding of computers and computer forensics; and second, to prevent future injustice wherever we are able".

[178] In primo grado, Trib. Vigevano, 17 dicembre 2009 il cui testo integrale di ben 158 pagine è reperibile nel sito dell'Ansa http://www.ansa.it/documents/1268750606840_SENTENZA_STASI.pdf, ed in Appello.

case inerenti omicidi senza colpevole, oltre a materiale inerente il profilo psicologico dei pedofili che potrebbe essere ricollegato a quello perdopornografico che "sembra" sia transitato sul pc del "fidanzatino di Garlasco".

17. Informatica e prevenzione dei reati

"Signor Marks, in nome della sezione precrimine di Washington
la dichiaro in arresto per il futuro omicidio
di Sarah Marks e Donald Dubin,
che avrebbe dovuto avere luogo oggi,
22 aprile alle ore 8 e 04 minuti"
dal film *Minority Report*

Sino ad ora si è visto come un computer possa essere rilevante ed a volte determinante nella fase di una indagine. Ma l'informatica può essere utile anche in una fase precedente il verificarsi di un crimine, se non addirittura per prevenire i reati in una sorta di sofisticato *Digital Profiling*. Ciò che viene raccontato in uno dei film più conosciuti nell'ambito della fantascienza, Minority Report, sta diventando realtà.

Già dal 2009 si è avuta notizia di esperimenti e progetti informatici in grado di operare nell'ambito di una sorta di "pre-crimine".

Il 23 giugno 2009, la polizia di stato presenta il nuovo organismo anticrimine: il CNAIPIC - Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche[179] con il compito di monitorare la rete al fine di prevenire gli attacchi informatici. L'attività svolta si focalizza soprattutto su reati informatici contro la sicurezza nazionale, la proprietà intellettuale e la *privacy*.

Nel 2010 viene data notizia di un *software* dell'IBM che sfruttando le potenzialità dell'analisi predittiva, giunge a prospettare delle vere e proprie zone calde dove i crimini potrebbero verificarsi. Questo grazie all'incrocio di dati inerenti a delitti, posizione geografica, persino alle previsioni metereologiche (sembra appurato che in caso di pioggia durante la notte, si rubino più auto), a furti e ad atti vandalici commessi dai criminali già noti alla polizia.

Il programma si chiama CRUSH - Criminal reduction utilising statistical history[180]) ed il suo *test* dura ormai dal 2006, anno in cui fu utilizzato per la prima volta in USA, precisamente nel Tennessee presso la città di Memphis,

[179] Cfr. www.poliziadistato.it/articolo/15664-infrastrutture_critiche_vita_dura_per_gli_hacker/.

[180] La traduzione è: "Riduzione del crimine utilizzando memorie statistiche".

dove, a detta della stessa Polizia il *software* ha di fatto contribuito alla diminuzione di alcuni crimini[181]. Ora sembra sia stato dato alla polizia britannica ed è in uso solo presso alcune sezioni che lo stanno sperimentando.

Nel 2011 il New York Times[182] ha dato notizia di un altro progetto, questa volta sperimentato dalla polizia di Santa Cruz, che sta sviluppando un *software* straordinario, in grado di elaborare dei dati ed ipotizzare quali reati saranno commessi in un determinato giorno, in un determinato orario ed in una determinata località. Le potenzialità del *software* sono state confermate da successi e riscontri positivi. Ciò che contraddistingue questo *software* da tanti altri simili utilizzati dalle polizie statunitensi è il fatto che si basa sui modelli usati per prevenire i terremoti e, dunque, è in grado di creare delle proiezioni sulle aree maggiormente a rischio.

Il DHS - Department of Homeland Security sta testando un *software*, il FAST - Future Attribute Screening Technology, pensato per scoprire le persone che hanno intenzione di commettere un atto terroristico. In questo caso il *software* agisce come una macchina della verità ma "a distanza", perché si basa su sensori senza contatto. Il programma sarebbe in grado di giungere a determinate deduzioni in seguito all'analisi di indicatori legati agli atteggiamenti (ad esempio il modo di camminare) di una persona. In questo caso la questione si fa ancora più interessante perché l'utilizzo di un simile *software* potrebbe confliggere con i princìpi legati alla *privacy*.

A livello europeo abbiamo il nostro caso, che è noto come INDECT, una sorta di pre-crimine europeo. Un ambizioso sistema di monitoraggio. Nella home page del sito[183] si legge "The INDECT Project aims at developing tools for enhancing the security of citizens and protecting the confidentiality of recorded and stored information"[184]. Il progetto è stato avviato nel 2009 e si prevede che si concretizzerà nel 2014, secondo una stima approssimativa. Tra i sostenitori e fautori il PSNI - Police Service of Northern Ireland, e molti ricercatori di varie Università (polacche, spagnole, britanniche, austriache, tedesche, bulgare) oltre ad aziende europee. INDECT rientra in un ambito di progettazione più vasto che persegue una cooperazione tra le polizie europee.

[181] Il 31% tutti i tipi di crimine ed il 15% dei crimini di tipo violento.

[182] La notizia nel sito della testata http://www.nytimes.com/2011/08/16/us/16police.html?_r=4.

[183] http://www.indect-project.eu/.

[184] "Il Progetto INDECT si propone di sviluppare strumenti per migliorare la sicurezza dei cittadini e proteggere la riservatezza delle informazioni registrate e archiviate".

In tutti questi casi è emerso come l'uso di *software* di questo tipo possano presentare non pochi problemi, primo fra tutti il conflitto con il principio della presunzione d'innocenza. Dall'altro lato gli aspetti positivi sono indubbiamente molti. In questo modo si supererebbe, infatti, la normale fase della reazione all'evento criminale, in cui il reato si è già verificato, per giungere a quella più positiva della prevenzione dell'evento dannoso, fase in cui il reato non si è ancora verificato e probabilmente non si verificherà mai. In questo caso, inoltre, i vantaggi ottenuti sono sia di tipo economico sia di sicurezza pubblica[185].

In realtà questi *software* di forte ausilio per gli investigatori sono una applicazione di sistemi già conosciuti come *data mining*, da tempo utilizzati nel marketing. Nella previsione del crimine il database utilizzato gestisce come dati le informazioni legate ad eventi criminosi che opportunamente analizzati conducono alla formulazione di conseguenze razionalmente prevedibili[186]. Ciò che si intende ottenere attraverso un DM (*data mining*) è la creazione di strumenti in grado di trasformare i dati in vere e proprie informazioni utili che nel caso dei reati, non sono più rivolte ad arginare o combattere i crimini bensì tendono a prevederli evitando che si concretizzino. D'altra parte occorre ricordare che il diritto non è nuovo a queste forme di "contaminazione" delle tecnologie soprattutto se si fa riferimento ai sistemi esperti applicati al settore giuridico.

18. Etica professionale e computer forensic

"Non penso mai al futuro. Arriva così presto"
Albert Einstein

La *computer* ed *information ethics* viene definita, illustrata e percepita come quella branca dell'etica applicata che studia e analizza gli impatti sociali ed etici della *Information and Communication Technology*[187].

[185] Ad esempio la polizia di Edmonton, in Canada, utilizza tecnologie di analisi realizzate da IBM per ridurre la criminalità, aumentare l'efficienza del corpo di polizia e rafforzare la sicurezza pubblica, in http://www.ibm.com/.

[186] Le analisi ed i collegamenti dei dati permetterebbero così la modellazione delle relazioni o comunque dei rapporti prevedendo i comportamenti di potenziali clienti o utenti. In questo caso di criminali.

[187] G. Ziccardi, *Etica e informatica. Comportamenti, tecnologie e diritto*, Milano, Pearson, 2009.

I princìpi etici sono spesso insiti in ciascun individuo e si manifestano nella diversità di pensiero e di ideologia che governano le vite dei singoli soggetti; si sostiene infatti che l'etica è dentro le persone e che sia impossibile trasmettere princìpi morali diversi da quelli provenienti dalla famiglia, dalla religione, dalla società ovvero dal bagaglio culturale e dall'esperienza acquisita da ciascuno.

Questo emerge chiaramente se si osservano le difficoltà che il legislatore incontra ogni qual volta si deve confrontare con normative di notevole valore etico (procreazione, aborto, testamento biologico, sperimentazione ecc. ecc.). Sono leggi che spesso divengono oggetto di democrazia diretta, referendum, che scontentano inevitabilmente parte della società, e per le quali sovente si chiedono modifiche attraverso nuovi disegni di legge.

È evidente quindi che l'esperienza vissuta e acquisita da ognuno sarà probabilmente diversa da quella dell'altro ed andrà a formare il vissuto etico di ciascuno.

Proprio per raggiungere una convivenza comune all'interno delle società, sarà opportuno darsi delle regole comportamentali da seguire nel rispetto reciproco, che non assumeranno valore normativo e non rientreranno nella gerarchia delle fonti giuridiche, ma avranno l'arduo compito di dettare princìpi comportamentali per un gruppo di persone.

Può avvenire che gli individui, in contatto con situazioni in cui è richiesta una decisione di natura etica, si trovino a dover gestire e affrontare un possibile conflitto tra il proprio credo e quelli dell'organizzazione, della società, dell'attività lavorativa; ciò non significa che si debbano abbandonare i propri princìpi e soggiacere a valori in contrasto con il proprio ideale. Esistono casi di obiezione di coscienza che permettono ai soggetti di astenersi dal comportamento in conflitto con la propria personalità, casi comunque rari, regolati da normativa apposita e per situazioni di una certa gravità etica/comportamentale[188].

Sovente i codici etici sono regolamenti scritti e depositati che i soggetti appartenenti ad una data categoria si danno con lo scopo di agevolare e regolamentare il proprio settore di appartenenza. Le professioni intellettuali, ad esempio, hanno una lunga storia in merito ai propri codici etici (es. del medico, dell'avvocato, dell'architetto), emanati dalla federazione nazionale

[188] Cfr. art. 16, l. 22 maggio 1978, n. 194 in G.U. 140 del 22 maggio 1978 "Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza"; art. 16, l. 19 febbraio 2004, n. 40 "Norme in materia di procreazione medicalmente assistita" in G.U. 45 del 24 febbraio 2004.

"articoli/devivo" — 2012/4/5 — 10:45 — page 110 — #110

della categoria e riconosciuti dallo Stato. Altre volte i codici etici sono delle regole non scritte ma seguite dagli utenti.

Anche gli utilizzatori del *web* hanno regole etiche non scritte ma che dovrebbero seguire nell'utilizzo del pc, attraverso princìpi validati e procedure corrette.

Un professionista che svolga la propria attività in *computer forensic* non dovrebbe mai dimenticare che sussiste in capo alla sua attività il segreto professionale che assume nei confronti della clientela, dovendo assolutamente evitare la divulgazione di informazioni acquisite durante l'indagine.

Altro requisito essenziale è l'acquisizione dei dati; ci sono procedure e standard etici che devono essere seguiti nell'acquisizione della prova, nella sua conservazione e nella messa a disposizione di chi ha commissionato l'indagine (difensore, magistrato, PM ecc).

Risulta essere essenziale la conservazione delle prove poiché l'eventuale manomissione o deterioramento provoca il loro non utilizzo. Le prove raccolte dovrebbero essere integrate con la data, l'ora e il luogo dove sono state trovate.

Successivamente si passa all'analisi delle prove in modo tale da eliminare quelle che non possono essere prodotte in tribunale. Il passo successivo di un comportamento etico comprende la presentazione delle prove in tribunale e la messa a disposizione delle parti in causa.

È altresì necessario che, dopo l'analisi dei risultati, i dati vengano restituiti al legittimo proprietario; ciò costituisce l'ultima parte nel comportamento etico nella *computer forensic*, previo consenso del magistrato.

Abbandonando l'ambito strettamente professionale di chi svolge la propria attività in *computer forensic*, si analizza ora l'utente medio del *web*, ovvero colui che popola l'agglomerato virtuale più numeroso del mondo con i suoi comportamenti più o meno etici.

Con il termine "Netiquette" ovvero il Galateo *on-line* (dall'unione di Net ed Etiquette) si intende quell'insieme di regole di comportamento che dovrebbero guidare l'uso della rete, comprendendo la posta elettronica, i messaggi pubblicitari, gli *spam*.

Entrando in Internet si accede ad un mondo libero e gratuito dove ciascuno deve rispettare e conservare le risorse di rete e rispettare gli altri utenti. Poiché non c'è una autorità che possa concretamente redarguire immediatamente i comportamenti scorretti *on-line*, sarebbe essenziale che ciascuno degli utenti si comporti con responsabilità rispettando il mondo virtuale utilizzando semplicemente il buon senso.

"articoli/devivo" — 2012/4/5 — 10:45 — page 111 — #111

Da quanto analizzato nei capitoli precedenti si rileva però che sebbene molti utenti rispettino e seguano comportamenti corretti, esiste un discreto numero di utenti che invece usano la rete per compiere azioni devianti. La conseguenza di ciò sarà che si arriverà a restrizioni inevitabili e a controlli, fino alla prospettazione dell'autodistruzione della rete.

Sarebbe opportuna l'esistenza di un codice di autodisciplina che possa almeno indicare quali sono i comportamenti altamente sanzionabili nel momento in cui non ci sia ragionevolezza nell'uso della rete da parte degli utenti.

Si riportano i dieci comandamenti nell'uso della rete come redatti dal CPSR - Computer Professionals for Social Responsibility[189]:

- non userai un computer per danneggiare altre persone;
- non interferirai con il lavoro al computer di altre persone;
- non indagherai nei *file* di altre persone;
- non userai un computer per rubare;
- non userai un computer per portare falsa testimonianza;
- non userai o copierai *software* che non hai dovutamente pagato;
- non userai le risorse di altri senza autorizzazione o compensazione corretta;
- non ti approprierai del risultato del lavoro intellettuale altrui;
- penserai alle conseguenze sociali dei programmi che scrivi;
- userai il computer in un modo che mostri considerazione e rispetto per le creature umane.

Sebbene siano regole scarne ed elementari, si possono reputare assolutamente utili per un corretto uso della rete.

Analizzando il punto 3 che vieta l'intromissione in *file* di altre persone, appare evidente come si possa agevolmente superare l'apparente contrasto con l'attività investigativa di *computer forensic*, bilanciando gli interessi in gioco. L'investigatore che analizza i *file* di un soggetto indagato ha come scopo l'individuazione del reo e/o l'interruzione di reati commessi a mezzo Internet. Non sussiste dunque alcun contrasto con i comandamenti etici del decalogo.

[189] CPSR is a global organization promoting the responsible use of computer technology. Founded in 1981, CPSR educates policymakers and the public on a wide range of issues. CPSR has incubated numerous projects. Originally founded by U.S. computer scientists, CPSR now has members in 26 countries on six continents (http://cpsr.org/issues/ethics/cei/).

"articoli/devivo" — 2012/4/5 — 10:45 — page 112 — #112

Volendo ultimare il discorso di natura etica professionale, si deve notare che ogni professione presenta delle caratteristiche raccolte in un corpo sistematico e unitario di teorie e conoscenze, con un organismo istituzionale ed indipendente dallo Stato che controlla e verifica l'esercizio delle conoscenze stabilendo le condizioni e gli scopi dell'attività professionale e al tempo stesso ha il diritto e il dovere di giudicare i suoi membri, sia sotto il profilo tecnico che etico[190].

Gli operatori della *computer forensic* si dovranno dotare, in un prossimo futuro, di linee guida ben precise fino ad arrivare ad un vero e proprio codice deontologico, ciò a causa dell'ambito delicato in cui operano sia nel reperimento che nella conservazione della prova, professionalizzando sempre più la loro attività.

In merito all'etica che dovrebbe avere ciascun utente della Rete, questo aspetto sarà molto più complicato, in quanto, come poc'anzi affermato, i comportamenti rispecchiano il proprio credo, di conseguenza ci sarà chi, comportandosi correttamente, non creerà alcun problema altrui, diversamente coloro i quali avranno atteggiamenti sconsiderati nella Rete andranno a colpire la collettività fino all'ipotesi peggiore di soppressione dei rapporti *on-line*, come da sempre avviene nei regimi totalitari e nelle rivolte popolari in cui, come prima conseguenza di repressione, si vedono oscurate le linee di comunicazione[191].

[190] M. TAVANI, M. PICOZZI, G. SALVATI, *Manuale di deontologia medica*, Milano, Giuffrè, 2007, pp. 7-10.

[191] L'Egitto torna *on-line*. In questi cinque giorni di buio digitale, solo le "vecchie" BBS e un *workaround* di *Google* e *Twitter* avevano offerto agli egiziani una "finestra sul mondo digitale". Ora si riaccende Internet in Egitto. Dopo aver spento Internet costringendo 4-5 Isp al *black-out* nazionale, l'Egitto si riaffaccia sul *web*. Lo riporta Renesys. Succede all'indomani di una manifestazione oceanica contro Mubarak e dopo l'invito di Obama a dare una svolta al regime e di aprire le porte alla democrazia. In questi cinque giorni di buio digitale, solo le "vecchie" BBS e un escamotage ingegnoso di Google e *Twitter* (un *workaround* per inviare *file* audio da telefono fisso sul *micro-blogging*) avevano offerto agli egiziani una "finestra sul mondo digitale" (Mirella Castigli, L'espresso, 2 febbraio 2011) consultabile anche in http://www.itespresso.it/legitto-torna-online-50182.html.