UNIVERSITA' DEGLI STUDI DI CATANIA

DIPARTIMENTO DI GIURISPRUDENZA

XXV CICLO DEL DOTTORATO DI RICERCA IN POLITICHE EUROPEE DI DIRITTO PROCESSUALE, PENALE E DI COOPERAZIONE GIUDIZIARIA

LE INTERCETTAZIONI TELEMATICHE NEL SISTEMA DELLE INVESTIGAZIONI DIGITALI

DOTTORANDO:
DOTT. FRANCESCO LO IACONO

COORDINATORE:
CHIAR.MA PROF.SSA ANNA MARIA MAUGERI
UNIVERSITA' DEGLI STUDI DI CATANIA

TUTOR:
CHIAR.MA PROF.SSA VANIA PATANE'
UNIVERSITA' DEGLI STUDI DI CATANIA

INDICE

Capitolo III:
Le intercettazioni del voip.

PREMESSA

L'evoluzione scientifica e tecnologica degli ultimi decenni ha radicalmente rivoluzionato le molteplici forme di interazione tra persone, potenziandone la velocità di trasmissione del pensiero e fornendo strumenti di azione e comunicazione dotati di incredibile efficacia. La crescente rilevanza che in un mondo sempre più interconnesso e globalizzato ha assunto, in particolare, la comunicazione informatica e telematica, ha reso non più rinviabile la previsione di norme volte, da un lato, a tutelarne la libertà e segretezza – così come richiesto e prescritto dalla Costituzione - e, dall'altro, a regolamentarne in modo più incisivo ed efficace le differenti forme di intrusione (o il loro utilizzo a fini criminali) oltre che la necessaria captazione a fini investigativi.

Le variegate forme di comunicazione per via informatica e telematica – nell'ambito degli eterogenei rapporti interpersonali di tipo ludico, commerciale, amministrativo ma anche, ovviamente, criminale – hanno ormai raggiunto, dopo anni di straordinaria espansione e diffusione, un ruolo centrale ed irreversibile nella società contemporanea, di talché una piena conoscenze delle problematiche giuridiche e tecniche sottese a tali realtà deve ritenersi bagaglio ormai indispensabile anche nell'ambito della generalità delle investigazioni penali. In questo senso l'informatica non può più essere considerata esclusivamente un modo di organizzazione e scambio di idee e beni, quanto piuttosto il linguaggio tipico della peculiare società nella quale viviamo, essendo infatti il dialogo di diretta percezione sensoriale tra persone ormai frequentemente surrogato dalla connessione telematica tra reti di elaboratori.

Le predette connessioni informatiche e telematiche risultano peraltro sempre più frequentemente utilizzate (proprio per le loro intrinseche caratteristiche di velocità di trasmissione e possibilità di totale crittazione) nell'ambito di attività od operazioni riferibili a differenziati e pericolosi contesti criminali.

Di ciò si è reso conto molto presto il legislatore italiano che, intervenendo nello specifico settore con norme di inusitata lungimiranza e modernità, ha cercato di conferire sistematicità e coerenza ad una materia oltremodo delicata e complessa.

Il differenziato e separato impianto normativo destinato ad illustrare e disciplinare puntualmente la (relativamente) recente categoria dei reati informatici risale, infatti, ai primi anni '90 del secolo scorso, quando, all'unisono con l'introduzione dei *cc.dd. computer crimes* (noti, altresì, come *cybercrimes*) nel codice penale (l. 23/12/1993, n.547), il legislatore decise di inserire nel sistema una prima peculiare forma di ricerca, raccolta e disamina della prova digitale: *la captazione telematica* (prevista, ancor oggi, dall'art.266 bis c.p.p.). Da quel momento si è potuto assistere ad un susseguirsi di innesti normativi, non sempre peraltro confinati nell'alveo del codice di rito, che portano, oggi, alla individuazione di un sistema non sempre organico, ma sufficientemente coerente e strutturato e comunque tale da poter vantare una parziale emancipazione dai binari ordinari del procedimento penale.

Il conseguente diffondersi di forme speciali nell'agire processuale - come ampiamente si sottolineerà all'interno di questo lavoro - ha assunto progressivamente i contorni di un vero e proprio "sottosistema". Quest'ultimo peraltro non è soltanto volto alla ricostruzione processuale degli illeciti informatici *stricto sensu*, ma è divenuto distintivo di tutte quelle situazioni in cui, più in generale, la macchina giudiziale sia costretta a fare i conti con un corredo probatorio avente matrice digitale. È il caso, ad. esempio, dei processi riguardanti reati comuni perpetrati con strumenti elettronici e, con sempre maggior frequenza, dei giudizi che, pur attinenti a condotte del tutto svincolate da ogni dimensione tecnologica, debbano confrontarsi con prove a carico (ma anche a discarico) immagazzinate, sottoforma di dati, all'interno di un elaboratore elettronico, di una rete, di una qualunque memoria di massa o, comunque, caratterizzate da una connotazione di tipo informatico o digitale.

Ancora, l'evoluzione storica che dal primo (citato) esperimento normativo ha condotto sino alle più recenti riforme organiche, nel suo dipanarsi, si caratterizza per la persistenza di un preciso *leit motiv*: la rinuncia cioè (quasi integrale) da parte del legislatore a creare nuovi istituti processuali in favore di un'espansione o di un riadattamento di istituti tradizionali, all'uopo riplasmati sulla cangiante realtà fenomenica. Si tratta di un percorso che trova il proprio paradigma più nitido proprio nella legge 18 marzo 2008 n.48 che, per l'appunto, si è in larga misura limitata a "sdoppiare" elementi già esistenti nell'ordinamento, affiancando, ad esempio, alla perquisizione locale tradizionale una perquisizione informatica e, parallelamente, alla classica ispezione dei luoghi, un'ispezione informatica.
Le tappe di questa ideale parabola legislativa meritano peraltro di essere sinteticamente rammentate.

Le fasi più significative, dunque, del lungo percorso che conduce fino all'attuale assetto della disciplina cui ci si riferisce possono essere ricollegate, a partire dal già richiamato intervento del 1993, essenzialmente e convenzionalmente, a tre importanti stagioni riformatrici. *In primo luogo* quella della **legislazione repressiva della pedopornografia *on line*,** collocandosi nella seconda metà degli anni '90 (l. 15.02.1996 n.66, e soprattutto la l. 03.08.1998 n.269) - con una appendice dalle ricadute maggiormente sostanziali, a circa dieci anni di distanza (l. n.38 del 2006) - contraddistinta da una germogliazione di metodi investigativi *ad hoc* (siti civetta, attività di contrasto in rete, operazioni sottocopertura) e da un impulso verso più sofisticate forme di organizzazione e specializzazione della polizia giudiziaria. Le predette normative, o meglio gli espedienti di natura sostanziale e procedurale predisposti dal legislatore nazionale per stigmatizzare e reprimere condotte ritenute particolarmente biasimevoli e perciò meritevoli di severe sanzioni, hanno trovato

peraltro puntuale riscontro in ambito internazionale, venendo portati ad ulteriori sviluppi, dalla Convenzione di Lanzarote[1].

In seconda battuta, si rinviene il periodo delle **leggi antiterrorismo** successivo all'abbattimento delle torri gemelle, con il suo apparato di disposizioni d'ampliamento dei controlli sulle comunicazioni anche in via preventiva (l.15 dicembre 2001 n.438 e d.l. 7 luglio 2005 n.144) e l'influsso sul *c.d. codice privacy* (l. 30.06.2003 n.196) soprattutto in materia di *data retention;* questione cruciale, quest'ultima, divenuta oggetto nel corso degli anni di molteplici modificazioni e continui aggiustamenti (l. 26 febbraio 2004 n. 45; l. 31 luglio 2005 n. 155; d.lgs. 30 maggio 2008 n. 109) probabilmente anche in virtù delle incisive sollecitazioni comunitarie in punto di protezione dei dati personali (cfr. da ultimo la direttiva 2006/24/CE)[2].

Infine, terza ed ultima fase, il tentativo (non sempre riuscito e mai comunque definitivamente abbandonato) di sistematizzazione, *ratione materiae*, lungo il solco tracciato dalla Convenzione di Budapest del 2001 emanata nel contesto del Consiglio d'Europa e sfociata nella citata **l. n. 48 del 2008**: novella, quest'ultima, essenzialmente diretta ad imprimere una svolta organica al settore tramite, in primo luogo, il rimodellamento e l'aggiornamento di svariate fattispecie penali sostanziali (quali falsità informatiche, delitti contro la sicurezza dei dati e dei sistemi informatici ecc. ecc.); quindi, attraverso il ripensamento delle attività urgenti della P.G. e di alcuni mezzi di ricerca della prova (ispezioni, perquisizioni e sequestri), per finire con l'allargamento dello spettro della responsabilità degli enti ex d.l. 8 giugno 2001 n.231 all'insieme degli illeciti informatici.

È da questo coacervo di normative che occorre, quindi, prendere l'abbrivio al fine di ricomporre in modo del tutto organico e coerente il quadro di riferimento, tenendo peraltro in debita considerazione, altresì, i provvedimenti eccentrici rispetto ai tre archi di tempo individuati (si pensi, solo per fare alcuni esempi, alla legge 20 novembre del 2006 n.281, in punto di intercettazioni telematiche illegalmente formate ovvero alla legge n° 12 del 15 febbraio 2012 in tema di confisca obbligatoria dei beni e degli strumenti informatici utilizzati, in tutto o in parte, per la commissione di un c.d. *cybercrime*) e, soprattutto, le divaricazioni dai normali *standard* del

[1] *Convenzione del Consiglio d'Europa del 2007 per la protezione dei minori contro ogni forma di abuso e di sfruttamento sessuale.* La convenzione è stata recepita nell'ordinamento italiano con la recente legge 1 ottobre 2012 n°172.

[2] Si ritiene peraltro, alla luce dello scandalo sorto durante l'estate 2013 in seguito alle rivelazioni da parte di Edward Snowden - un ex consulente della americana NSA (*National Security Agency*) che ha svelato l'esistenza di un intenso programma di controllo di massa delle comunicazioni posto in essere dai governi di U.S.A. e UK (al quale, da quanto risulta, avrebbero collaborato, seppur parzialmente, anche altri 6 Stati della U.E.) – che nuove iniziative legislative potrebbero essere intraprese nel breve/medio termine dalle Istituzioni europee nella specifica materia dei *data retention*.

processo derivanti tanto dalle prassi forensi[3], tipiche del particolare campo di indagine, quanto dalla accentuata singolarità della criminalità informatica.
In questo settore, più ancora che in altri ambiti, quindi, come acutamente evidenziato da autorevole dottrina, sono proprio le "*peculiarità oggettive e soggettive dei fatti da accertare"* a modellare il rito *"secondo profili spesso inediti o comunque sensibilmente originali"*[4].

[3] Si pensi, ad esempio, al complesso di protocolli, linee guida e direttive che, *de facto,* si sono andati stratificando e consolidando nei dettami e nei (frequentemente stringenti) precetti apportati dalla c.d. *computer forensic.*

[4] Così Amodio, *I reati economici nel prisma dell'accertamento processuale,* in Riv. It di diritto e preoc pen, 2008, 1499

Capitolo I: Le intercettazioni telematiche ed informatiche nell'ordinamento processuale italiano.

***

"... intercettare è
ascoltare, possibilmente senza essere ascoltati..."
(Cordero F.)

1.1 La tutela costituzionale delle comunicazioni.

1.1.a) La tutela interna.

In una risalente sentenza della Corte Costituzionale[5] viene chiaramente affermato il principio secondo il quale le speciali garanzie predisposte dalla legge *"a tutela della segretezza e della libertà di comunicazione telefonica* - si ricordi che nel 1993 le tecnologie telematiche preordinate a specifiche finalità di comunicazione cominciavano a diffondersi in modo ancora estremamente elitario – *rispondono all'esigenza costituzionale per la quale l'inderogabile dovere di prevenire e reprimere i reati deve essere svolto nel più assoluto rispetto di particolari cautele dirette a tutelare un bene,* ***l'inviolabilità della segretezza e della libertà delle comunicazioni****, strettamente connesso alla protezione del nucleo essenziale della dignità umana e al pieno sviluppo della personalità delle formazioni sociali (art. 2 della Costituzione)".*
In una pronuncia ancor più risalente[6], perlatro, il Giudice delle leggi, in termini decisamente più ampi ed astratti, evidenzia chiaramente come il contenuto dei diritti primari e fondamentali non possa, per ciò solo, considerarsi privo di limiti, sottolineando che l'art. 2 Cost., *"nell'affermare i diritti inviolabili dell'uomo e i doveri inderogabili di solidarietà politica, economica e sociale, non può escludere che a carico dei cittadini siano poste quelle restrizioni della sfera giuridica rese necessarie dalla tutela dell'ordine sociale",* anche se i diritti connotati dalla inviolabilità *"essendo intangibili nel loro contenuto di valore, possono essere unicamente disciplinati da leggi generali che possono limitarli soltanto al fine di realizzare altri interessi costituzionali altrettanto fondamentali e generali"*[7].
Dette restrizioni – afferma ancora la Corte[8] - sono necessarie poiché *"i diritti primari e fondamentali dell'uomo diverrebbero illusori per tutti, se ciascuno potesse esercitarli fuori dell'ambito della legge, della civile regolamentazione, del costume corrente, per cui tali diritti devono venir contemperati con le esigenze di una*

[5] Corte Cost.le Sent. n. 81 del 1993.
[6] Corte Cost.le Sent. n. 75 del 1966.
[7] Corte Cost.le Sent. n. 235 del 1988.
[8] Corte Cost.le Sent. n. 168 del 1971.

tollerabile convivenza" e la regola da seguire, affinché tali limiti siano ammissibili, è quella della ***"necessarietà e ragionevolezza della limitazione***[9]**".**

In questa prospettiva, rispetto alla **libertà e alla segretezza delle comunicazioni** garantite dalla Carta Costituzionale**,** la Corte ha sottolineato che *"la stretta attinenza di tale diritto al nucleo essenziale dei valori di personalità – che inducono a qualificarlo come parte necessaria di quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana – comporta una* ***duplice caratterizzazione della sua inviolabilità****. In base all'****art. 2 della Costituzione****, il diritto a una comunicazione libera e segreta è inviolabile, nel senso generale che il suo contenuto essenziale non può essere oggetto di revisione costituzionale, in quanto incorpora un valore della personalità avente un carattere fondante rispetto al sistema democratico voluto dal costituente. In base all'****art. 15 della Costituzione****,* d'altra parte, *lo stesso diritto è inviolabile nel senso che il suo contenuto di valore non può subire restrizioni o limitazioni da alcuno dei poteri costituiti se non in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante, sempreché l'intervento limitativo posto in essere sia strettamente necessario alla tutela di quell'interesse e sia rispettata la duplice garanzia che la disciplina prevista risponda ai requisiti propri della riserva assoluta di legge e la misura limitativa sia disposta con atto motivato della autorità giudiziaria*[10]*".*

Questa, quindi, la cornice Costituzionale di riferimento all'interno della quale collocare il complessivo sistema di garanzie e tutele in relazione ai peculiari strumenti investigativi sui quali ci si concentrerà nel prosieguo della trattazione. L'inevitabile estensione legislativa del concetto di comunicazione a tutte le forme di trasmissione di dati in forma digitale, pertanto, determina l'operatività anche per le stesse, della tutela prevista dall'**art. 15 della Costituzione** che, come indicato *supra*, definisce *"inviolabili" "la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione"* e ne consente la limitazione *"soltanto per atto motivato della A.G. con le garanzie stabilite dalla legge".*

Il Costituente ha inteso, quindi, apprestare una tutela particolarmente rafforzata per questa fondamentale libertà, imponendo una duplice *riserva*: di "*legge"* e di "*giurisdizione".* Secondo autorevole dottrina, peraltro, la prima, delle due anzidette riserve, avrebbe addirittura una valenza ed una portata significativamente più rigorose rispetto alla (medesima) riserva posta a presidio della libertà personale, di stampa e di domicilio, avendo ritenuto il legislatore di non derogarne l'operatività – neppure in eccezionali ipotesi di *necessità* ed *urgenza* – non attribuendo in alcun caso alla P.G., diversamente da ciò che accade per le precedenti libertà (anche quella personale!) – tutte parimenti garantite dalla Costituzione - il potere di porre in essere, *motu proprio,* interventi limitativi, in assenza di un provvedimento *ad hoc* della A.G.

[9] Corte Cost.le Sent. n.141 del 1996.
[10] Corte Cost.le Sent. n.366 del 1991.

In maniera sicuramente condivisibile, quindi, il legislatore ordinario ha ritenuto non assimilabili – e quindi non sovrapponibili ai fini della specifica disciplina normativa - le due espressioni *"con le garanzie stabilite dalla legge",* adoperata dall'art. 15 Cost. e *"nei soli casi e modi stabiliti dalla legge",* di cui all'art 13 Cost. (cui fra l'altro rinvia l'art. 14 Cost.). Questa impostazione è stata peraltro condivisa ed avallata dalla Corte Costituzionale che, in una famosa sentenza del 1973[11] ha sottolineato come il difficile contemperamento tra tutela della libertà e segretezza delle comunicazioni, da un lato, ed esigenza di prevenire e reprimere i reati, dall'altro, non può non trovare esplicazione nella puntuale e dettagliata disciplina che li legislatore deve predisporre al fine di regolamentare le concrete modalità (tecniche ed operative) attraverso le quali i servizi di intercettazione debbono essere predisposti, assicurando stabilmente alla A.G. la possibilità di effettuare una penetrante e pronunciata attività di controllo (non soltanto di matrice giuridica, bensì, come si vedrà in seguito, anche sugli apparati e le materiali tecnologie di captazione utilizzate nell'ambito del singolo procedimento[12]).

1.1.b) La tutela sovranazionale

Le precedenti considerazioni trovano, in linea di massima, ampio e puntuale riscontro nel diritto internazionale, prevalentemente pattizio, avendo da tempo la disciplina convenzionale assunto il compito di proclamare e promuovere il rispetto dei **diritti umani,** a cominciare dagli irrinunciabili e connessi aspetti di tutela attinenti alla libertà personale, domiciliare e, per quanto di interesse in questo lavoro, di comunicazione.

Nello specifico, procedendo in modo estremamente schematico e sintetico (ma non per questo meno puntuale), la libertà e la segretezza di ogni forma di comunicazione è principio apertamente e solennemente sancito da numerose ed importanti fonti di rango sovranazionale ed internazionale, quali:

- **la "Dichiarazione Universale dei Diritti dell'Uomo" (art.12);**
- **la "Convenzione Europea sui Diritti dell'Uomo" del 1950 (art.8);**
- **il "Patto sui diritti civili e politici", adottato dall'ONU il 16.12.1966** (reso esecutivo con la L.881 del 1977);
- **la "Carta dei diritti fondamentali dell'UE", approvata dal Consiglio europeo di Nizza nel 2000 (art.7)** (che dopo l'entrata in vigore del Trattato di Lisbona - ufficialmente il 1 dicembre 2009 – ha assunto dignità e valore giuridico pari a quella dei trattati sull'U.E. e sul Funzionamento della U.E.)**.**

L**'art. 8 par. 1 C.e.d.u.** statuisce che *«ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza»*.

[11] Corte Cost.le Sent. n. 34 del 1973

[12] Da qui la differente disciplina ed i conseguenti contrasti interpretativi aventi ad oggetto l'art. 268, co.3° e co. 3° bis del C.p.p. - relativi all'utilizzo degli impianti installati presso gli uffici delle Procure della Repubblica, sui quali cfr. *infra*).

Benché la norma *de qua* non accordi ad esse diretta ed esplicita protezione, non pare revocabile in dubbio che le comunicazioni informatiche e telematiche - ed in generale tutte le molteplici forme di comunicazione – rientrino appieno nella tutela apprestata alla persona attraverso i concetti di *«vita privata»* e di *«corrispondenza»*[13].

Sul punto, peraltro, la giurisprudenza della Corte europea dei diritti dell'uomo appare pacifica.

Ed in questo senso, a parere dei giudici di Strasburgo, ogni tipo di intercettazione *«riveste di per sé la caratteristica di ingerenza della pubblica autorità nella sfera privata* e ciò, anche quando *«di essa non si sia fatto un uso processualmente rilevante»*[14]. Parimenti tutelata peraltro è, nell'ottica della Corte, la rilevazione *«di ogni altro elemento relativo alla conversazione», di tal ché si ravviserebbe «una violazione della vita privata»* anche laddove l'informativa fosse limitata al rilevamento di dati quali l'ora, la durata della comunicazione o il numero composto dal chiamante[15].

Pacifico appare per di più il fatto che la locuzione *«persona»* ricomprenda in sé *«anche gli enti e le associazioni che il soggetto crea e che, di poi, assumono autonomo rilievo nella società ove vivono ed operano»*:[16]. Di qui, la considerazione in base alla quale, se è pur vero che, con riguardo alle persone giuridiche, l'intromissione possa avvenire *«con margini più ampi rispetto alle limitazioni delle persone fisiche»*, l'attività posta in essere *«deve comunque sempre presentare adeguate garanzie contro eventuali abusi»*[17].

Non meno importanti sono le previsioni contenute nell'**art. 8 par. 2 C.e.d.u.** secondo il quale *«non può aversi interferenza di una autorità pubblica nell'esercizio del diritto* (al rispetto della vita familiare, del domicilio e della corrispondenza) *a meno che questa ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la sicurezza pubblica, per il benessere economico del paese*[18]*, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà degli altri».*

---

[13] Zeno Zencovich, Art. 8, in AA.VV., *Commentario alla Convenzione per la tutela dei diritti dell'uomo e delle libertà fondamentali,* a cura di S. BARTOLE – B. RAIMONDI – G.CONFORTI, Padova, 2001, 307 e ss.

[14] Corte e.d.u., caso Kopp c/Svizzera, 25 marzo 1998. Nello stesso senso, Corte e.d.u., caso Ludi c/Svizzera, 15 giugno 1992.

[15] Questo orientamento sarà ripreso *infra* allorquando si affronterà la tematica dell'acquisizione dei dati esteriori delle comunicazioni (*c.d. blocco*) ex art. 4 l. n. 675 del 1996 riprodotto nell'art. 132 del codice della privacy. Per quanto concerne poi i profili prettamente giurisprudenziali, si segnala la pronuncia Corte e.d.u., caso H. c/Repubblica Ceca, 1°marzo 2007, secondo la quale, *«in tema di acquisizione di tabulati telefonici, anche il mero elenco cronologico delle chiamate tra più utenze ricadono sotto la protezione dell'art. 8 C.e.d.u.: come tali, l'acquisizione degli stessi in un processo penale costituisce ingerenza nella vita privata».*

[16] Furfaro*, Un problema irrisolto: le intercettazioni telefoniche, in Procedura penale e garanzie europee, Torino, 2006, 120.*

[17] Corte e.d.u., caso Stés Colas Est c/Francia, 16 aprile 2002.

[18] In proposito, si vedano Corte e.d.u., caso M.S. c/Svezia, 27 agosto 1997, nonché, Corte e.d.u., caso Ciliz c/Paesi Bassi, 11 luglio 2000.

Con riguardo a detta riserva di legge, si è autorevolmente osservato in dottrina che i diversi modi di produzione normativa propri degli Stati contraenti impongono di rapportare detto concetto alle esigenze di concretezza e di effettività che animano la Convenzione[19]. Il testo inglese di essa, del resto, utilizzando l'espressione generica *«in accordance of the law»*, non intende richiamare un preciso procedimento di produzione normativa, quanto piuttosto il concetto di diritto, in modo che ogni decisione dei giudici e le loro motivazioni possano essere prevedibili almeno nelle linee essenziali.
Tanto il Costituente quanto le norme sovranazionali sopracitate – sancito il formale ed indefettibile riconoscimento della piena libertà e segretezza di tutte le indistinte forme di comunicazione, quali appartenenti al nucleo essenziale degli imprescindibili diritti democratici - presuppongono, quindi, l'esistenza di un'area di disvalore penale per l'accertamento e la repressione della quale le intercettazioni – nel senso più ampio e generale possibile - si presentano come uno strumento dal quale oggi non si può assolutamente prescindere.
Semplificando si potrebbe a ragione considerare l'esistenze delle intercettazioni negli ordinamenti democratici come un vero e proprio *bug*[20] (iniziando così a prendere familiarità con espressioni, in seguito, ampiamente utilizzate) rispetto ai principi di Democrazia e alle teorie generali di fondo; ciononostante, è opinione ormai universalmente accolta che, se di *male* si vuol per forza parlare, le stesse (intercettazioni) costituiscono, ad una più approfondita considerazione, un "male" inevitabile e per molteplici aspetti assolutamente necessario.

1.2 La disciplina codicistica.

1.2.a) Generalità

Nel diritto processuale penale italiano, l'intercettazione viene annoverata tra i mezzi di ricerca della prova *tipici*, previsti e disciplinati cioè dal legislatore e, segnatamente, dagli articoli 266 e ss. del codice di procedura penale.
In termini molto generali[21], l'art. 266 stabilisce, al primo comma, che l'intercettazione di conversazion comunicazioni telefoniche e di altre forme di telecomunicazione sono consentite nei procedimenti relati specifiche fattispecie di reato (non così, come si vedrà *infra,* per le intercettazioni telematiche, l'esperibilità delle quali non si prevede alcuna elencazione tassativa di ipotesi delittuose).

[19] Furfaro, *op.* cit.
[20] In termini informatici, l'espressione *bug* (in italiano baco) identifica un errore nella scrittura di un programma software. Meno comunemente, il termine bug può indicare un difetto di progettazione in un componente hardware, che ne causa un comportamento imprevisto o comunque diverso da quello specificato dal produttore.
[21] Nel trattare tali disposizioni si manterrà, anche in seguito, un approccio estremamente generalistico, lasciando pertanto maggior spazio e risalto alle questioni di più stretta attinenza rispetto al presente lavoro.

Dal punto di vista empirico, le intercettazioni consistono nel complesso di attività ed operazioni dirette a captare comunicazioni e conversazioni, nonché, per quanto di maggiore interesse ai nostri fini, **flussi di comunicazioni informatiche o telematiche (art. 266 bis c.p.p.),** mediante gli strumenti approntati, in un dato momento storico, dalla tecnica.
Come accennato precedentemente, l'intercettazione tende a limitare gravemente alcune importanti libertà costituzionali, per cui il legislatore ha stabilito particolari norme procedurali volte a garantire la legittimità formale e sostanziale delle pertinenti attività[22]. Il codice di procedura penale, conseguentemente, prevede specifici limiti e presupposti ed in generale una disciplina procedimentale estremamente rigorosa. Infatti, oltre ai precedenti presupposti oggettivi inerenti il **reato per cui si procede**, è necessario che sussistano gli ulteriori presupposti oggettivi dei **gravi indizi di reato** e della **assoluta indispensabilità** dell'intercettazione ai fini della prosecuzione delle indagini.

1.2.b) I Presupposti.

Quanto ai presupposti procedurali ed esecutivi ai fini dell'esperibilità delle intercettazioni, si registra tradizionalmente, in dottrina e giurisprudenza, assoluta unanimità di visione circa la sussumibilità tanto delle intercettazioni di conversazione quanto di quelle informatiche e telematiche ai medesimi "requisiti" contemplati dall'**art. 267 c.p.p**.. Per un verso è il legislatore stesso a lasciarlo agevolmente presupporre nel momento in cui interviene ad interpolare[23] la disciplina prevista dall'art. 268 e mostrando implicitamente di non voler delineare *ex novo* una procedura specifica per le suddette intercettazioni[24]; per altro verso, invece, sono imprescindibili ragioni di ordine logico e sistematico ad imporlo. Se così non fosse, infatti, l'unica soluzione, nel silenzio della legge, sarebbe unicamente quella di ipotizzare intercettazioni informatiche sganciate da qualsiasi limite e presupposto, ma vincolate al rispetto delle formalità esecutive di cui all'art.268 c.p.p. *"E si tratterebbe di una soluzione non solo palesemente assurda, ma anche apertamente contrastante con il citato disposto dell'art. 15 della Costituzione…".*[25]

1.2.c) I gravi indizi di reato e l' indispensabilità ai fini delle indagini.

[22] Nel pieno rispetto sia della riserva assoluta di legge sia della riserva di giurisdizione, entrambe contemplate espressamente dalla Costituzione.
[23] Con l'art. 12 della L. 23 dicembre 1993 n. 547 che ha per l'appunto introdotto nel nostro ordinamento la figura delle intercettazioni di comunicazioni informatiche e telematiche.
[24] Così ad es. Parodi, *La disciplina delle intercettazioni telematiche*, in Criminalità informatica 2008, pp 889 ss
[25] C. Di Martino, *Le intercettazioni telematiche e l'ordinamento italiano: una convivenza difficile,* Indice Penale 2002, pp.221 e ss.

Punto di partenza dell'analisi è che i **gravi indizi** che, ai sensi dell'art. 267, comma 1, c.p.p. costituiscono presupposto per il ricorso alle intercettazioni, attengono alla mera esistenza del reato e non (come pure nel passato si è tentato di far pensare) alla colpevolezza di un determinato soggetto (obiettivo dell'intercettazione[26]); per procedere ad intercettazione non e' pertanto necessario che i detti indizi siano a carico dei soggetti le cui comunicazioni debbano essere, ai fini investigativi, intercettate[27].

Altro presupposto normativo, non alternativo bensì giustapposto ai gravi indizi di reato, è costituito dalla **indispensabilità** delle intercettazioni ai fini delle indagini.

Va ancora precisato che il requisito dei gravi indizi di reato deve essere inteso non in senso probatorio (ossia come valutazione del fondamento dell'accusa), bensì *come vaglio di particolare serietà delle ipotesi delittuose configurate*, *che non devono risultare meramente ipotetiche, con la conseguenza che è da ritenere legittimo il decreto di intercettazione telefonica disposta nei confronti di un soggetto che non sia iscritto nel registro degli indagati*[28]. Da tale principio, la Suprema Corte ha fatto discendere il corollario in base al quale *"la mancata individuazione dell'autore dell'illecito in relazione al quale è disposta la intercettazione influisce sulla utilizzabilità dei suoi effetti nello stesso procedimento ai fini di prova di condotte criminose collegate"*[29].

Alla stregua dell'orientamento prevalente in giurisprudenza, il requisito della indispensabilità delle intercettazioni (che, ai sensi dall'art. 267 comma 1, deve essere assoluta) ai fini della prosecuzione delle indagini, può essere valutato esclusivamente dal giudice di merito, la cui decisione può essere censurata, in sede di legittimità, solo sotto il profilo della manifesta illogicità della motivazione[30].

Sotto questo profilo, merita peraltro di essere ricordato, incidentalmente, come le intercettazioni derivanti da decreti non motivati (o comunque inutilizzabili) possono nondimeno presentare una loro utilità ai fini del procedimento. La giurisprudenza infatti, unanimemente, ritiene che esse possano costituire *notitia criminis* ai fini dell'espletamento di nuove attività di indagine, potendosi porre per di più a presupposto di nuove e diverse intercettazioni, motivandone la sussistenza degli indizi alla luce del contenuto delle intercettazioni inutilizzabili[31].

Si è osservato in proposito che in materia di inutilizzabilità non trova applicazione il principio di cui all'art. 185 cpp secondo il quale la nullità dell'atto rende invalidi gli atti consecutivi che da quello dichiarato nullo dipendono[32] ed inoltre che la operatività della garanzia di inutilizzabilità dei mezzi probatori illegittimi e' riservata

---

[26] In questo senso l'art.11 del DDL n. 1611 di riforma di tutta la materia delle intercettazioni approvato dal Senato il 10 giugno 2010

[27] Cass. Sez. VI, 18 giugno 1999, n. 9428, Patricelli; Sez. V, 7 febbraio 2003, n. 38413, Alvaro e altri.

[28] L'assunto è stato ribadito, sia pure con riferimento al vaglio dei decreti autorizzativi nel procedimento diverso da quello nel quale sono stati emessi, dalle SS.UU. 17 novembre 2004, n. 45189, Esposito.

[29] Sez. I, 3 dicembre 2003, n. 16779, Prota.

[30] Sez. VI, 25 settembre 2003, n. 49119, Scremin.

[31] In questo senso, ex multis, la sent Cass. sez. I, 2.3.2010, n. 16293 e la ancora più recente Cass sez. II, 4.I.2012 n.64;

[32] Sez. III, 29 aprile 2004, n. 26112, Canaj, rv 229058.

al momento giurisdizionale, da intendersi non solo come fase dibattimentale, ma come ogni fase o sede nella quale il giudice assume le proprie decisioni; pertanto le informazioni (assunte attraverso mezzi di prova illegittimi e perciò) inutilizzabili per il giudice, possono essere utilizzate legittimamente dal pubblico ministero e dalla polizia giudiziaria per il prosieguo delle indagini[33].

Ulteriore conferma di questo univoco indirizzo interpretativo consolidatosi nella giurisprudenza della Suprema Corte è offerto da quella sentenza emessa a Sezioni Unite in cu il giudice di legittimità, ribaltando il precedente orientamento prevalente, ha statuito la assoluta inutilizzabilità dei risultati di qualsivoglia tipo di intercettazione (telefonica, informatica o ambientale) anche nell'ambito del giudizio (innanzi al giudice civile) volto ad ottenere la riparazione per ingiusta detenzione.[34]

Con un'altra recente interpretazione - anch'essa evidentemente volta alla massima salvaguardia delle acquisizioni investigative - i Giudici con l'ermellino, da ultimo, hanno altresì statuito che sono da considerarsi pienamente utilizzabili anche quelle intercettazioni disposte legittimamente per uno dei reati indicati dall'art. 266 c.p.p., qualora dalle stesse emergano altri reati e purché gli stessi siano "soggettivamente ed oggettivamente collegati o connessi" con il primo reato (quello nell'ambito del quale sono state disposte le intercettazioni), e ciò anche nell'ipotesi in cui il reato o i reati (soggettivamente ed oggettivamente) collegati non rientrino tra quelli per i quali la legge prevede l'esperibilità del peculiare strumento di ricerca della prova (ad esempio perché puniti con pena edittale inferiore, nel massimo, ai cinque anni di reclusione)[35].

In un caso che non ha mancato di suscitare qualche perplessità tra i commentatori[36], la Corte di Cassazione ha ritenuto pienamente utilizzabili - in un differente procedimento (ex art. 600 quarter c.p. *detenzione di materiale pedopornografico*) - le acquisizioni derivanti dalle intercettazioni telematiche disposte nell'ambito di un procedimento ex art. 600 ter c.p. (*pornografia minorile*) instaurato nei confronti di altro indagato. In particolare, dette acquisizioni indussero il P.M. a disporre una perquisizione nei confronti di altro soggetto con la conseguente sottoposizione a sequestro di materiale pornografico avente ad oggetto minori. In questo caso la Corte ha argomentato asserendo che in base al noto principio *" male captum bene retentum",* trattandosi di cose obiettivamente sequestrabili e suscettive di confisca obbligatoria il provvedimento ablatorio era da considerarsi pienamente legittimo.

Sempre in tema di utilizzabilità delle intercettazioni – più specificamente sotto il profilo concernente l'utilizzazione in altri procedimenti (art. 270 c.p.p.) – è opinione ormai largamente consolidatasi (anche con riferimento alle intercettazioni informatiche e telematiche) che *"i risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti, salvo che*

[33] Cass. Sez. III, 10 febbraio 2004, n. 16499, Mache, rv 228545

[34] Cass. SS.UU. 30 ottobre 2008, n. 1153.

[35] Cass., sez. VI Penale, sentenza n. 34735/11 del 26 settembre 2011.

[36] Cass. Sez. III sent. n.42113 del 21.12.2006.

risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza"[37].

Sul punto va segnalato che, con il medesimo intervento, le Sezioni Unite della Corte di Cassazione, hanno escluso che tra le cause di inutilizzabilità delle intercettazioni in altro procedimento vi sia il mancato deposito dei relativi decreti autorizzativi: *"Ai fini dell'utilizzabilità degli esiti di intercettazioni di conversazioni o comunicazioni in procedimento diverso da quello nel quale esse furono disposte, non occorre la produzione del relativo decreto autorizzativo, essendo sufficiente il deposito, presso l'Autorità giudiziaria competente per il "diverso" procedimento, dei verbali e delle registrazioni delle intercettazioni medesime*).

1.2.d) La disciplina speciale: sufficienti indizi di reato e mera necessità ai fini delle indagini.

E' noto che il legislatore del 1991[38] ha attenuato i presupposti legittimanti il ricorso allo strumento delle intercettazioni per **indagini su "delitti di criminalità organizzata o di minaccia col mezzo del telefono"**, prevedendo che l'intercettazione non sia "indispensabile", ma semplicemente *"necessaria"* per le anzidette indagini e richiedendo al contempo indizi (rispetto a detti reati) non "gravi", ma solo *"sufficienti*". Deroghe notevoli attengono anche alla durata delle operazioni (40 giorni per la prima attivazione e 20 per ogni proroga [anziché 15 per la prima attivazione e 15 per ogni proroga]).

La disciplina in esame è stata estesa[39] altresì ai procedimenti per i delitti di cui all'art. 407 comma 2 lett. a) n. 4 c.p.p. (delitti con finalità di *terrorismo* o di *eversione dell'ordinamento costituzionale* con pena non inferiore nel minimo a 5 anni o nel massimo a 10 anni, delitti di cui all'art. 270 comma 3, 270 bis comma 2, 306 comma 2, cod. pen.) e per il delitto ex art. 270-ter cod. pen. (*Assistenza agli associati nei reati di associazione sovversiva e di associazione con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico*). I presupposti in parola si applicano poi[40] alle intercettazioni relative ai procedimenti per i delitti previsti dagli artt. 600-604 cod. pen. (*Riduzione in schiavitù; Prostituzione minorile; Pornografia minorile; Detenzione di materiale pornografico; Iniziative turistiche volte allo sfruttamento della prostituzione minorile; Tratta e commercio di schiavi; Alienazione e acquisto di schiavi*) e per i delitti di cui all'art. 3, l. 20 febbraio 1958, n. 75 (c.d. legge Merlin).

---

[37] Cass. S.U. n°45189 del 17.11.2004.

[38] Art. 13 d.l. 13 maggio 1991 n. 152 conv. in l. 12 luglio 1991, n. 203, successivamente modificato dall'art. 3-bis d.l. 8 giugno 1992, n. 133 conv. in l. 7 agosto 1992, n. 356 e da ultimo dall'art. 23 l. 1° marzo 2001, n. 63

[39] Art. 3, comma 1, d.l. 18 ottobre 2001, n. 374, conv. in l. 15 dicembre 2001, n. 438.

[40] In virtù dell'art. 9 l. 11 agosto 2003 n. 228.

Ciò detto, la norma peraltro non chiarisce se la possibilità di disporre intercettazioni nei termini (più agevoli) previsti dallo stesso art. 13 L 203/91 sia estensibile anche alle intercettazioni informatiche e telematiche di cui all'art. 266-bis c.p.p.; la questione è di non poco momento, in quanto proprio la diffusione delle comunicazioni digitali – spesso, come si vedrà nel prosieguo, criptate - nell'ambito della criminalità organizzata, anche internazionale, risulta ormai un fenomeno statisticamente rilevante (si pensi soltanto alle transazioni monetarie eseguite elettronicamente).

Ragioni sistematiche e teleologiche, quali la priorità della lotta alla criminalità organizzata, potrebbero invero supportare la tesi della applicabilità delle citate deroghe anche alle intercettazioni telematiche ed informatiche, considerato anche che il richiamo all'art. 266 c.p.p. potrebbe essere letto in riferimento a tutti i tipi di intercettazioni previste dall'ordinamento al momento di entrata in vigore della Legge 203/1991 (essendo state introdotte le intercettazioni telematiche nel nostro sistema giuridico soltanto due anni dopo). In questo senso la l. 547 del 1993, lungi dal prevedere una disciplina "speciale" rispetto all'art. 266 c.p.p., si sarebbe limitata unicamente ad integrare le disposizioni in materia di intercettazioni.

Una tale interpretazione estensiva non può, tuttavia, considerarsi autorizzata dalla lettera della norma, che fa appunto esclusivo riferimento all' *"autorizzazione a disporre le operazioni previste dall'art.266 dello stesso codice".* E ciò anche alla luce del fatto che, proprio in tema di lotta alla criminalità organizzata, l'art. 13 della legge 547/1993 si è invece premurato ad estendere la disciplina prevista dalla L. 7 Agosto 1992 n°356 sulle c.d. *intercettazioni preventive* (*infra*) anche al *"flusso di comunicazioni relative a sistemi informatici o telematici"*[41]. In ultima analisi, l'indicata lacuna normativa dovrebbe rientrare, a rigore - attesa la potenza precettiva dell'art. 15 della Costituzione – nel novero di quelle che all'interprete non è dato colmare.

Secondo il prevalente (antitetico) approccio interpretativo[42], viceversa, è all'identità di *ratio* che caratterizza l'operatività dei due diversi strumenti di ricerca della prova che si deve guardare. Poiché l'art.266 bis consente l'espletamento delle intercettazioni informatiche e telematiche *"nei procedimenti relativi ai reati indicati nell'art. 266 c.p.p.";* atteso che i delitti di criminalità organizzata rientrano nel novero delle fattispecie criminali per le quali il legislatore ammette il ricorso alle captazioni ex art.266, sarebbe del tutto illogico ed irrazionale non estendere le previsioni derogatorie (all'art. 267 c.p.p.) di cui al prefato art. 13 della L.203 del 1991 anche alle intercettazioni telematiche. Ma non solo. Aderendo all'opposto orientamento, si verrebbe a determinare un'insensata ambiguità del dato normativo che, rispetto al

[41] Non ci si spiega, invece, per quale ragione il legislatore non abbia avvertito la medesima esigenza di allargare esplicitamente l'ambito di operatività della norma, anche con riferimento alla possibilità di attenuare il vigore dei presupposti per il ricorso alle intercettazioni telematiche, con riguardo peraltro alle medesime ipotesi delittuose

[42] In questo senso: Camon op. cit. pg.12; Parodi, La disciplina delle intercettazioni telematiche, op. cit. pg 892; Fumu, op. cit.; Balducci, Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria; Aprile- Spiezia, Le intercettazioni telefoniche ed ambientali, Milano 2004;

medesimo fatto criminale (fra l'altro caratterizzato dall' accentuato allarme sociale) ed a parità di intrusività dei due strumenti, adotterebbe due pesi e due misure.
Sulla nozione di **"criminalità organizzata"**, per finire, si è soffermata recentemente una importante pronuncia delle Sezioni Unite[43]. Dalla decisione in parola si desume agevolmente come la Corte abbia ritenuto che nel procedimento penale rimesso al suo esame - relativo fra l'altro ad imputazione ai sensi dell'art. 416 cod. pen. - l'appello che il P.M. aveva presentato al Tribunale della libertà (così dando luogo alla ordinanza oggetto di ricorso per cassazione) fosse inammissibile, non operando per la fattispecie associativa la sospensione dei termini durante il periodo feriale, a norma dell'art. 2 comma 2 l. n. 742 del 1969.
Atteso che la menzionata sospensione dei termini delle indagini preliminari nel periodo feriale non opera nei processi per "reati di criminalità organizzata", la decisione della suprema Corte si è verosimilmente fondata sull'assunto implicito che il procedimento sottoposto al suo esame (instaurato, come sottolineato precedentemente, per il reato di cui all'art. 416 c.p.) dovesse fruire del regime previsto dall'art. 2 comma 2 l. cit., ossia quello derogatorio (per il quale non opera appunto la sospensione dei termini) essendo anche l'associazione per delinquere volgarmente definita "semplice" fattispecie rientrante nella nozione di "reato di criminalità organizzata".[44.]
Così statuendo la Suprema Corte ha posto termine ad un annoso ed irrisolto contrasto giurisprudenziale, prevedendo finalmente anche per i reati ex art. 416 c.p. la possibilità di far ricorso, durante la fase delle indagini preliminari, allo strumento delle intercettazioni (telefoniche, informatiche o cc.dd. "ambientali") alla stregua di presupposti derogatori, meno stringenti e rigorosi, rispetto a quelli contemplati dall'art. 267 C.p.p. .

1.3 L'art. 266 bis c.p.p

1.3.a) La legge n°547 del 23 dicembre 1993: le intercettazioni informatiche e telematiche.

Mosso dalla consapevolezza che le organizzazioni criminali mostrano sempre accentuato interesse verso tutti i nuovi portati della tecnica che consentono comunicazioni rapide, efficienti ed altamente sicure[45] e spinto dalla necessità di coordinare le prime disposizioni codicistiche dettate in materia di criminalità informatica con il vigente sistema processuale, il legislatore italiano pensò di

[43] SS.UU. 22 marzo 2005, Petrarca, n. 17706.
[44] Non potendo, cioè, il P.M. calcolare il termine per la impugnazione, avvantaggiandosi della sospensione estiva dei termini procedurali, la sua impugnazione avrebbe dovuto essere considerata tardiva.
[45] Questo aspetto verrà ampiamente approfondito i*nfra* (Capitolo III "le intercettazioni del c.d.voip").

intervenire su quello che, tra i mezzi di ricerca della prova, è da considerarsi ontologicamente più aperto alle innovazioni tecnologiche: le intercettazioni.

Nacquero così le intercettazioni informatiche (o, più esattamente, delle *comunicazioni informatiche e telematiche*) come si legge nella rubrica dell'art. 266 bis del codice di procedura penale, introdotto dall'art. 11 della legge n°547 del 23 dicembre 1993.

La disciplina delle nuove tipologie di intercettazioni venne per molti aspetti modellata su quella delle intercettazioni ordinarie[46], prevedendo però al contempo anche una serie di aspetti normativi ed operativi del tutto autonomi e pertanto di specifico interesse ermeneutico.

Nella L. 547/93 l'informatica, per la prima volta, non viene più considerata unicamente come uno dei tanti modi di organizzazione, gestione e condivisione di idee, conoscenze, beni e servizi, quanto piuttosto il linguaggio "tipico" ed universale della società nella quale viviamo. Cosicché una piena conoscenza delle problematiche giuridiche e tecniche ad essa sottese viene improvvisamente ritenuta bagaglio indispensabile nell'ambito delle investigazioni penali.

Questo radicale mutamento di prospettiva trova puntuale riscontro, in prima battuta, nelle numerose ed "inedite" fattispecie criminali che il legislatore italiano - al fine di adeguarsi alla Raccomandazione del Consiglio d'Europa R(89) 9 del 13 settembre 1989[47] - battendo (inopinatamente) sul tempo la stragrande maggioranza degli altri paesi aderenti, inserisce nell'alveo della sua principale fonte di diritto criminale: il Codice Penale.

Invero, già agli inizi degli anni '90 dello scorso secolo (*sic!*), la diffusione degli strumenti informatici aveva comportato rilevantissime trasformazioni sociali, purtroppo non soltanto in senso positivo. Il mondo criminale, infatti, come accennato sopra, aveva da tempo intuito la possibilità di avvalersi del mezzo operativo informatico a fini illeciti. Inoltre, cominciò a diffondersi una forma delinquenziale del tutto nuova, quella cioè degli *hacker*[48] che, mossi dalla volontà di dimostrare la propria abilità (e, quindi, per una sorta di gioco o di sfida) ovvero per il desiderio di affermazione personale da raggiungere attraverso la realizzazione di atti clamorosi, tali da riscuotere un'elevata rilevanza nell'ambiente informatico o sui *mass media,* agivano (e agiscono) senza altri fini se non quello di introdursi all'interno di sistemi informatici altrui e, solitamente, danneggiarli.

---

[46] Quelle cioè contemplate dagli artt. 266 e ss. c.p.p. e delle quali si sono accennate alcune peculiarità nei paragrafi precedenti di questo stesso capitolo.

[47] In relazione alla quale cfr Sarzana, Informatica e diritto penale, Milano, 1994, 247

[48] Il termine nasce con l'informatica ed è rivolto ad identificare chi attacca strumenti informatici col solo scopo di capirli e smontarli, senza arrecare danno o sottrarre informazioni. Il termine deriva dal verbo inglese *"to hack"* che appunto significa scomporre, ridurre in parti funzionali. A rigore, quindi, il c.d. *hacker* deve essere tenuto debitamente distinto dal *cracker* il cui scopo intrusivo principale (in un sistema informatico) trova finalità eminentemente nell'intento di distruggere ovvero di appropriarsi di dati informatici altrui. Il verbo *to crack* significa appunto distruggere. Anche il legislatore criminale non ha, per la verità, tenuto in debito conto la diversità essenziale corrente tra queste figure effettivamente affini sanzionandone le condotte in modo uguale (cfr. para. 2.2 *infra*).

Furono pertanto, da un lato, inserite nel codice nuove e fino a quel momento, inedite, fattispecie delittuose, dall'altro, talune già esistenti furono novellate. Questi, i reati che furono oggetto di intervento della legge 547/93: l'accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.); la detenzione e diffusione abusiva di codici di accesso a sistemi informatico o telematici (art. 615 quater c.p.); la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.); il danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.); la frode informatica (art. 640 ter c.p.); l'attentato ad impianti di pubblica utilità (art. 420 c.p.); la falsità di documenti informatici (art. 491 bis c.p.); ed infine le previsioni ex artt. 617 quater, quinquies, sexies ed ex art. 616 c.p. a tutela delle comunicazioni informatiche e telematiche.
L'elencazione delle predette fattispecie non ha, ai nostri fini, una mera valenza tassonomica avendo, infatti, il legislatore del 1993 approntato lo strumento delle intercettazioni telematiche ed informatiche eminentemente (ma, non esclusivamente, come si vedrà *infra*) allo scopo di perseguire con più incisività ed efficacia proprio i nuovi reati previsti e sanzionati dalla legge n.547.

1.3.b) L'art. 266 bis c.p.p.: una disposizione necessaria.

A lungo si è discusso circa la necessità di introdurre nel codice di rito, tra gli strumenti di ricerca della prova, la specifica categoria delle intercettazioni di comunicazioni informatiche e telematiche.
Alcuni commentatori, già all'indomani della emanazione della l.547, non solo contestarono l'utilità della disposizione contenuta nell'art. 266 bis c.p.p., ma si spinsero addirittura a sottolinearne la perniciosità.
Sotto il primo profilo, fu rilevato come l'art. 266 c.p.p. non limitasse la sua previsione all'intercettazione di conversazioni o comunicazioni telefoniche, ma contenga già un, sia pur generico, riferimento ad *"altre forme di telecomunicazioni"* (art. 266 co.1 c.p.p.), si da consentirne un adattamento automatico ogniqualvolta ulteriori acquisizioni della scienza lo richiedessero. E siccome non può esservi dubbio che le comunicazioni telematiche rientrino nell'ambito delle *"altre forme di telecomunicazioni"* ecco dimostrata la superfluità della disposizione[49]. Prova ne sia che, anche prima dell'entrata in vigore della l. n. 547 del 1993, nessuno dubitava, ad esempio, della possibilità di intercettare le comunicazioni che avvenivano via fax.
Sotto il secondo profilo, e per conseguenza, veniva evidenziato come la manifesta lettura restrittiva del termine "telecomunicazioni" operata dal legislatore italiano nel 1993 recasse con sé la necessità di ulteriori, costanti interventi di riempimento ogniqualvolta la scoperta e l'impiego di una nuova tecnologia lo avessero reso

[49] In questo senso Fumu, sub art. 266 bis in Commento al codice di procedura penale, coordinato da Chiavario, Torino 1998

necessario, con il risultato di cancellare una delle più importanti innovazioni del vigente codice di procedura penale.
Le precedenti osservazioni, seppur suggestive, rischiano tuttavia di divenire capziose e non sembrano convincere fino in fondo.
E' vero, infatti, che ancor prima della emanazione della legge n.547 si faceva rientrare il concetto di intercettazione telematica, nel novero della disciplina delle intercettazioni di comunicazioni ex art. 266 co. 1 (ove appunto si parla di "altre forme di telecomunicazioni"), ma è altrettanto vero che detta sussunzione, oltre ad esporre ai "pericoli"[50] connessi all'estensione analogica delle norme in tema di intercettazione, dava luogo ad una equiparazione che appare immediatamente priva di fondamento qualora si proceda ad una analisi delle informazioni trasmesse via telefono, contrapponendole a quelle trasmesse via computer.
Le intercettazioni telefoniche consentono di inserirsi in una trasmissione "fonica" passante per una linea dedicata[51] o commutata[52]: sono, quindi, in grado di accertare che sia in corso una comunicazione, che ci sia uno scambio di impulsi tra modem. Non sono in grado però di decifrarne il contenuto. Ed è proprio per l'attività di decifrazione delle informazioni trasferite via modem che è stata predisposta l'intercettazione telematica: i suoni o gli impulsi trasmessi via computer vengono infatti intercettati e decifrati in informazioni interpretabili da un altro computer (a disposizione degli inquirenti) che le renderà comprensibili all'uomo.
Il precedente ragionamento è ancor più lapalissiano rispetto alle intercettazioni di comunicazioni "informatiche". Alla stregua dell'art. 266 c.p.p. esse non sarebbero state consentite. Dette intercettazioni, infatti, hanno ad oggetto più computer in grado di interagire tra loro senza avvalersi affatto dello strumento telefonico; si sarebbe trattato di una significativa limitazione, in quanto un singolo elaboratore può certamente "colloquiare" con altri attraverso un modem – e quindi avvalendosi del sistema telefonico – ma può altresì essere inserito in una LAN (*Local Area Network*), ossia nelle strutture ampiamente diffuse in enti pubblici e privati, in grado di organizzare e collegare dinamicamente fra loro varie postazioni di lavoro informatiche *(c.d. client)* in modo tale che le stesse possano elaborare e trasmettere dati, informazioni e programmi, attraverso particolari computer *(server)* diretti ad assicurare la funzionalità ed il coordinamento della rete. Ne consegue che, essendo la funzionalità di una LAN condizionata dall'utilizzo del sistema telefonico solo per porsi in connessione con realtà informatiche esterne alla rete locale, le intercettazioni in tale ambito (all'interno cioè del *Network*) sono possibili solo in forza del disposto dell'art.266 bis c.p.p. Ma anche nell'ipotesi in cui la LAN si ponesse in connessione con l'esterno, i normali mezzi di intercettazione telefonica, come detto, sarebbero unicamente in grado di registrare che è in atto una comunicazione via modem, non anche di decifrarne il contenuto. Se si vuole ottenere questo ulteriore risultato,

[50] In questo senso Sarzana *"La criminalità informatica: aspetti processuali"* in Quaderni del C.S.M., 1994 pg 348
[51] Un collegamento che unisce fisicamente due entità.
[52] Un collegamento fisico che unisce due entità tramite un commutatore.

pertanto, bisogna ricorrere, come già chiarito in precedenza, ad un computer programmato che decodifichi i suoni o gli impulsi intercettati, rendendoli intelligibili prima per se stesso e poi per l'uomo: occorre cioè porre in essere una specifica intercettazione telematica.

1.3.c) L'art. 266 bis: il difetto di tassatività.

Come si è detto *supra*, l'art. 15 della Costituzione, dopo avere proclamato inviolabili la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, ne consente tuttavia la limitazione purché con atto motivato dell'autorità giudiziaria e con le *garanzie stabilite dalla legge*. In ottemperanza a questo preciso dettato costituzionale - come riportato in precedenza - il legislatore, pur nella consapevolezza delle straordinarie potenzialità delle intercettazioni, ha ritenuto di dover circoscrivere entro precisi limiti il relativo potere delle autorità inquirenti, stabilendo in primo luogo, e *in maniera tassativa,* quali siano le fattispecie di reato per le quali è consentito il ricorso a questo mezzo di ricerca della prova (delitti puniti con l'ergastolo o la reclusione superiore nel massimo a cinque anni; delitti contro la Pubblica Amministrazione puniti con pena non inferiore a cinque anni; delitti in materia di stupefacenti, armi ed esplosivi; delitti di contrabbando, ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, manipolazione del mercato, pornografia minorile, anche cd. "virtuale").
L'art. 266 bis c.p.p., invece, afferma: "N*ei procedimenti relativi ai reati indicati nell'articolo 266 nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche è consentita l'intercettazione del flusso di comunicazioni...(omissis)".* Ora, mentre la prima parte della locuzione, mercé il rinvio all'articolo immediatamente precedente, non prospetta difficoltà interpretative, la seconda parte di essa fa sorgere notevoli dubbi. I *conditores,* ci si chiede, si sono voluti riferire esclusivamente ai reati dei quali l'impiego di tecnologie informatiche o telematiche sia *elemento costitutivo* ovvero anche a quelli di cui tale impiego costituisca soltanto una *modalità della condotta*?
Ancora una volta la dottrina si è trovata divisa. Parte di essa, sulla base del presupposto che la tassatività delle ipotesi in cui è consentita la violazione della segretezza delle comunicazioni non può non valere per tutte le "categorie" di intercettazioni, ritiene la scelta del legislatore chiaramente orientata nel senso di limitare l'uso delle (intercettazioni) informatiche all'accertamento di una determinata categoria di reati e la giustifica con la considerazione che, per assicurare alla giustizia i colpevoli di particolari tipi di reato - realizzabili soltanto grazie all'uso di strumenti informatici o telematici – è giocoforza violare la privacy delle comunicazioni che avvengono via computer, ma non occorre comprimere la libertà delle comunicazioni che vengono realizzate via telefono o altrimenti. La differenziazione operata dal legislatore sembra, dunque, legittimata dall'intento di circoscrivere al massimo le interferenze nelle comunicazioni altrui. *"D'altra parte - si prosegue - se si rifiutasse*

l'interpretazione restrittiva, si dovrebbe ammettere la legittimità dell'intercettazione informatica come mezzo di ricerca della prova per quei reati non compresi nell'elenco dell'art. 266 c.p.p. - per i quali, se non fossero realizzati con particolari moderne tecnologie, nessun altro mezzo di intercettazione sarebbe ammissibile. Si potrebbe ravvisare, allora, una disparità di trattamento (e dunque una violazione dell'art. 3 della Costituzione) tra i diversi imputati di uno stesso reato commesso con modalità tecniche differenti, le une legittimanti e le altre no l'intercettazione informatica: a parità di imputazione, infatti, l'inviolabilità delle comunicazioni sarebbe garantita solo se il reato fosse commesso senza l'uso di strumenti informatici"[53].

Tuttavia, ribattono altri, né la lettera né lo spirito della legge n. 547 del 1993 legittimano un'interpretazione restrittiva; le intercettazioni di cui all'art. 266 bis c.p.p. sono ammesse sia per i *reati informatici cd. propri* (quelli cioè in cui l'uso del computer è elemento costitutivo) sia per i *reati informatici impropri* (in cui l'uso del computer integra solo una delle modalità della condotta). Quanto, poi, alla pretesa disparità di trattamento fra imputati di uno stesso reato commesso con modalità tecniche differenti, paventata dai sostenitori dell'opposta tesi, essa è pienamente giustificata dalla maggiore pericolosità di cui è sintomo l'uso di un differente strumento che caratterizza la condotta[54].

L'opzione legislativa è stata pertanto ispirata dalla necessità di ampliare, *in subiecta materia,* le ipotesi di esperibilità del mezzo di ricerca della prova in oggetto, dovendosi prendere atto della impossibilità di controllare e reprimere seriamente determinate forme di criminalità senza ricorrere a siffatta, peculiare, forma di intercettazione delle comunicazioni. A tal fine, il legislatore ha dovuto garantire un ambito di operatività della disciplina in esame (certamente non tassativamente predeterminato) potenzialmente espandibile parallelamente al progresso scientifico e tecnologico.

Alla luce delle superiori considerazioni, è, allora, possibile tracciare il seguente quadro: a) quando le indagini hanno ad oggetto uno dei reati indicati dall'art. 266 c.p.p., sia o meno commesso con l'impiego di tecnologia informatica, l'autorità inquirente può ricorrere sia alle intercettazioni comuni sia a quelle informatiche; b) quando le indagini hanno ad oggetto reati diversi da quelli contenuti nell'elenco di cui all'art. 266 c.p.p., sono possibili solo le intercettazioni informatiche, sempre che i reati in questione siano stati commessi mediante l'uso di tecnologie informatiche o telematiche, anche se gli stessi non sono ricompresi nel novero dei *c.d. computer (o cyber) crimes,* vale a dire di quelle fattispecie introdotte dalla legge n°547 del 1993

---

[53] *Ugoccioni, sub art. 11 l. 23/12/1995 n°547 (Criminalità informatica), in LP, 1996, p.141*. In senso contrario Parodi *op. cit.* secondo il quale invece verrebbe garantito ossequio proprio all'art. 3 Cost. in quanto si porrebbe in essere una risposta adeguatamente differenziata a presupposti criminali certamente differenti.

[54] Questa seconda concezione ha trovato autorevoli sostenitori quali: Buonomo, in *AA.VV. Profili penali dell'informatica,* Milano 1994, pg. 135; ma anche Camon, *Le intercettazioni nel processo penale*, Milano, 1993, pg. 12 e ss.

così come implementate dalla legge n°48 del 18 Marzo 2008 di ratifica ed esecuzione della Convenzione di Budapest del 2001 sulla criminalità informatica[55].
In ragione di quanto appena affermato, per determinati illeciti informatici di gravità poco più che bagatellare sarà - ove ricorrano tutti i presupposti normativi - concedibile l'intercettazione telematica, ma non quella telefonica. Si tratta di una circostanza non priva di rilevo pratico, specie per l'attuale prassi investigativa, giacché alcune strumentazioni utilizzate per acquisire il flusso telematico possono contemporaneamente intercettare il traffico telefonico, sollevando forti dubbi di invalidità e quindi esponendo alla sanzione di inutilizzabilità (ex art. 271 c.p.p.) il complesso dei risultati acquisiti.
Infine, è evidente come l'opzione interpretativa dominante si mostra, nonostante le segnalate difficoltà interpretative, coerente, da un punto di vista sistematico, con quanto previsto dall'art. 266 c.p.p. Quest'ultima disposizione contempla infatti la possibilità di porre in essere intercettazioni (di conversazioni) – nel caso di reati perpetrati a mezzo telefono - non solo per delitti di non particolare allarme sociale (quale ad esempio l'ingiuria: co.1 lett. f) art.266 c.p.p.), ma addirittura per la contravvenzione di cui all'art. 660 c.p. *(molestia e disturbo delle persone)*, sulla base del solo presupposto che tali manifestazioni non possono essere fronteggiate se non ricorrendo allo specifico mezzo di ricerca della prova[56].

1.3.d) L'art. 266 bis: le norme "satellite".

Le intercettazioni informatiche non possono per ciò solo vivere di vita propria nel sistema; per funzionare e raggiungere lo scopo per il quale sono state introdotte necessitano, infatti, di una serie di apposite norme "satellite", stante la visibile inadeguatezza delle disposizioni dettate per le intercettazioni comuni. Proprio per questo il legislatore ha, per un verso, provveduto ad adattare, grazie a specifiche interpolazioni, la disciplina contenuta nei commi 6, 7 e 8 dell'**art. 268 c.p.p.** anche alle "nuove" intercettazioni; per altro verso, invece, ha provveduto ad inserire nello stesso articolo un **comma 3 bis** specificamente dedicato alle intercettazioni *de quibus*. Anche questo innesto ha recato non pochi problemi di coordinamento con le disposizioni già esistenti e, in particolare, come si vedrà diffusamente *infra*, con quella contenuta nel 3° comma del medesimo articolo.
Quanto agli aspetti più squisitamente processuali della materia, si noti come la novella del 1993, apportando come accennato alcune modifiche all'art. 268 c.p.p., sia riuscita ad adeguare la disciplina medesima alla particolare natura delle comunicazioni informatiche. Così:
- i difensori delle parti potranno prendere cognizione dei flussi di comunicazioni informatiche o telematiche;

[55] Su cui ci si soffermerà, senza eccessivi approfondimenti, *infra.*
[56] Come nota efficacemente Parodi, *La disciplina delle intercettazioni telematiche*, in Criminalità informatica 2003, a cura di Carlo Sarzana si Sant'Ippolito, pg. 889 e ss.

- il Giudice disporrà l'acquisizione delle conversazioni o dei flussi di comunicazioni informatiche o telematiche indicati dalle parti, che non appaiano manifestamente irrilevanti, procedendo anche d'ufficio allo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione;
- il Giudice, ancora, disporrà la trascrizione integrale delle registrazioni ovvero la stampa in forma intelligibile delle informazioni contenute nei flussi di comunicazioni informatiche o telematiche da acquisire, osservando le forme, i modi e le garanzie previsti per l'espletamento delle perizie.
- nel caso di intercettazione di flussi di comunicazioni informatiche o telematiche i difensori potranno richiedere copia su idoneo supporto dei flussi intercettati, ovvero copia della stampa prevista dal comma 7.

Al di là di questi "aggiustamenti", sono rimasti invece immutati - come evidenziato nel paragrafo *1.2.a)* - i cardini della sequenza procedimentale già prevista per le intercettazioni telefoniche *(necessità di gravi indizi circa la sussistenza di un reato; indispensabilità delle intercettazioni per la prosecuzione delle indagini; richiesta del Pubblico Ministero; autorizzazione del Giudice; previsione di un potere straordinario del Pubblico Ministero di disporre le intercettazioni nei casi di urgenza, salva convalida del Giudice; durata delle operazioni; svolgimento delle stesse da parte del Pubblico Ministero, con possibilità di delega alla Polizia Giudiziaria; tenuta dei registri delle intercettazioni, ecc.)*.

Va qui segnalato peraltro come le intercettazioni telematiche siano sovente disposte direttamente dal Pubblico Ministero; ciò in quanto le segnalazioni di reato in materia - specie con riguardo all'attività di posta elettronica o di "attacchi" a sistemi informatici - richiedono la massima rapidità nell'esecuzione di ricerca della prova, anche in ragione della estrema "volatilità" della tracce informatiche inerenti le attività criminose in oggetto.

In questo senso, la giurisprudenza si è più volte espressa per la legittimità di un decreto d'urgenza del Pubblico Ministero che pure non spieghi le ragioni della stessa urgenza, laddove siano ricavabili dalla peculiarità dei reati per cui si procede (*in re ipsa*). Esse possono infatti ritenersi implicitamente sussistenti – affermano i giudici di legittimità - quando si faccia risaltare la ritenuta esistenza di una attività criminosa in atto per la quale sussiste il dovere della PG di intervenire con la massima sollecitudine per impedire che essa venga portata a conseguenze ulteriori[57].

Infine, la giurisprudenza ritiene altresì estendibile alle intercettazioni telematiche il regime delle utilizzabilità scandito a proposito delle intercettazioni ordinarie (cfr. para. 1.2.c) *supra*). Così, laddove, ad esempio, esse possano assumere rilievo probatorio per l'accertamento di delitti per i quali è previsto l'arresto obbligatorio in flagranza ai sensi dell'art. 380 c.p.p., dette intercettazioni (telematiche e/o informatiche) effettuate sul solo presupposto dell'essere attinenti a reati commessi mediante l'impiego di tecnologie informatiche o telematiche, potranno essere

[57] Copiosa la giurisprudenza che ha seguito questo orientamento. Ex multis: Sez. V, 11 maggio 2004, n. 24241, Mancuso, rv 228107; Sez. VI, 21 gennaio 2004, n. 7691, Flori, rv. 229005; Sez. VI, 19 gennaio 2004, n.10777, Tassone, rv 229517; Sez. V, 27.09.2006 n. 36090, Santangelo

utilizzate in altri procedimenti. Ciò a condizione peraltro che i verbali e le registrazioni delle intercettazioni siano depositati presso l'autorità competente per il diverso provvedimento, con l'osservanza delle disposizioni di cui all'art. 268, 6°, 7°, 8° co., c.p.p.

1.3.e) L'utilizzo di impianti appartenenti a privati.

Come accennato nel paragrafo precedente, la modifica processuale forse più significativa rispetto ai modelli procedimentali preesistenti alla Legge 547/93 consiste nell'innesto del **comma 3-bis** nell'ambito dell'**art. 268 c.p.p.**, a mente del quale *"quando si procede a intercettazione di comunicazioni informatiche o telematiche, il pubblico ministero può disporre che le operazioni siano compiute anche mediante impianti appartenenti a privati".*

Si tratta di previsione che determina una possibilità espressa di deroga alla rigorosa disciplina prevista dall'**art. 268 co.3° c.p.p.**, che appunto impone che *le operazioni di intercettazione possano essere compiute esclusivamente per mezzo degli impianti installati presso la Procura della Repubblica,* ovvero - allorché *tali impianti risultino insufficienti od inidonei ed esistano eccezionali ragioni di urgenza* - mediante *impianti di pubblico servizio o in dotazione alla polizia giudiziaria,* con provvedimento "motivato" del Pubblico Ministero. La violazione di tale disposizione è sanzionata, ex art. 271 co.1°, c.p.p., con l'inutilizzabilità dei risultati delle intercettazioni medesime.

Di contro, il comma 3-bis dell'art. 268 non richiede alcun obbligo di motivazione, e soprattutto nessuno specifico presupposto per l'esecuzione delle operazioni con impianti diversi da quelli dell'Ufficio di Procura. Sostanzialmente, al PM è lasciata assoluta discrezionalità nell'uso degli impianti appartenenti a privati, trattandosi di strumenti ad alto "tasso" di tecnologia, di cui le Procure e gli Uffici di Polizia Giudiziaria non sono mai stati effettivamente dotati.

La previsione di un comma autonomo rispetto al comma 3 dell'art.268 c.p.p., consente quindi, in ossequio a criteri eminentemente pratici, di ritenere che la facoltà ivi prevista debba ritenersi del tutto autonoma e svincolata dai criteri previsti per l'utilizzo in generale di impianti di pubblica utilità ovvero della polizia giudiziaria, avendo verisimilmente il legislatore preso atto della cronica sottodotazione strutturale delle sedi giudiziarie oltre che della totale "assenza", al momento di entrata in vigore della legge, di idonee apparecchiature presso gli uffici normalmente deputati alle attività in oggetto.

Il ricorso agli impianti dei privati, pertanto, non costituirà affatto un'eccezione, ma semmai la regola per l'esecuzione di intercettazioni telematiche od informatiche.

In punto di motivazione la norma, come detto, nulla prevede. Per il disposto generale dell'art. 267,3° co., c.p.p., pertanto, al PM basterà indicare nel decreto "dispositivo" delle intercettazioni le "modalità" di esecuzione, senza che possa derivare alcuna sanzione processuale per il caso che ometta di motivarne la scelta.

Tuttavia, una parte della dottrina ritiene che la disposizione di cui al co.3 bis costituisca una mera prosecuzione del co. 3 dell'art. 268 e che le due norme si pongano l'una rispetto all'altra in rapporto di *species* a *genus*, sussistendo fra esse un collegamento non soltanto lessicale, ma anche logico[58]. Questa interpretazione troverebbe conferma nell'uso della congiunzione "anche" nel co.3 bis, che può essere agevolmente inteso nel senso che è diretto - fermi i presupposti previsti dal comma 3 - ad inserire un'ulteriore alternativa di fronte ad una situazione di impossibilità di utilizzare gli apparati della Procura. In questo senso, l'unica lettura consentita dei due commi in argomento, sarebbe quella "unitaria" che consentirebbe, fra l'altro, il necessario coordinamento della nuova disciplina con le norme concernenti i divieti di utilizzazione: cosicché, dalla violazione dei limiti posti all'utilizzazione di impianti privati per le intercettazioni telematiche ed informatiche deriverebbero le consequenziali sanzioni dell'inutilizzabilità dei risultati delle captazioni, e ciò benché l'art. 271 c.p.p. (in tema, appunto, di inutilizzabilità) non contenga alcun riferimento al co.3 bis - in questo senso cfr. Cass. Sez. I Sent. 28 settembre 1999 n°5239 che, in ossequio ai principi formulati in tema di intercettazioni dalla cit. Sent. Corte Cost.le, 4 aprile 1973 n. 34 (cfr. paragrafo 1.1.a), asserisce che il legislatore, nel regolamentare all'art.271 c.p.p. la sanzione processuale della inutilizzabilità del contenuto delle intercettazioni (norma, fra l'altro, entrata in vigore prima che venisse introdotto il comma 3bis) ha avuto presente non soltanto le captazioni di comunicazioni telefoniche, bensì quelle di ogni tipo di comunicazione, quali che siano le peculiari modalità di svolgimento.

Ancora, in un' importante pronuncia del Dicembre 2006[59], la Suprema Corte ha affermato il principio secondo il quale rientra nell'ambito operativo del comma 3° dell'art.268 c.p.p. (e non, quindi, del comma 3 bis) l'ipotesi in cui la P.G., autorizzata all'esecuzione di operazioni intercettative (telematiche/informatiche) mediante l'utilizzo di impianti diversi da quelli installati presso la Procura della Repubblica, vi provveda, utilizzando apparecchiature noleggiate da ditte private (o comunque in suo possesso a qualsiasi titolo ancorché appartenenti a privati) e ciò in quanto il comma 3 bis del citato articolo si riferisce esclusivamente al ricorso ad "impianti privati" i quali siano utilizzati direttamente dai medesimi soggetti privati nella loro veste di ausiliari tecnici del PM ovvero della P.G. e quindi sotto lo stretto controllo di quest'ultimi.

La situazione, quindi, è in tutto e per tutto analoga a quella in cui le operazioni di intercettazioni avvengano presso gli uffici della Procura, mediante l'utilizzo di impianti non appartenenti all'Amministrazione della Giustizia, bensì noleggiati da privati. Non vi sarebbe, evidentemente, nessun motivo per invocare, a tali condizioni,

---

[58] In questo senso ad es. Filippi, *L'intercettazione di comunicazioni*, Milano, 1997; GRIFFO, *Limiti all'integrazione del decreto adottato ai sensi dell'art. 268 comma 3*, nota a Cass. pen., Sez. Un., 29 novembre 2005, Campenni, in Cass. pen., 2006, 1347; Nevoli, *Intercettazioni informatiche e telematiche: ricorso ad impianti esterni ed obbligo motivazionale del P.M.* in Arch. Nuova Proc. Pen. 1/2010,76.

[59] Cass. Sez. II, 14.12.2006 n.14217, Calasso.

la disciplina derogatoria prevista dal codice di procedura, rispetto ad impianti sui quali il Magistrato possa comunque esercitare un controllo diretto e costante. Poderosa è la giurisprudenza della Suprema Corte stratificatasi su questo precipuo orientamento interpretativo[60].

A ben vedere, quindi, la vicenda in esame andrebbe ricondotta nell'alveo del comma 3 e non del comma 3 bis dell'art. 268 del c.p.p. con conseguente ed ineludibile obbligo motivazionale per l'Autorità Giudiziaria in punto di insufficienza e/o inidoneità degli impianti installati negli uffici della Procura. Va altresì messo in rilievo come il collegamento tecnico in questione - assicurato dal soggetto gestore tecnico del sevizio internet (Provider o Server) ed utilizzato dalla P.G. per le operazioni di captazione - consentirà quasi sempre, alla luce degli enormi progressi compiuti dalle tecnologie informatiche negli ultimi tempi (mediante l'uso ad es. di indirizzi e-mail creati ad hoc) la visualizzazione (ad es. sottoforma di e-mail) dei flussi intercettati, su comunissimi PC quali quelli in dotazione ad ogni magistrato del pubblico ministero.

1.3.f) Le intercettazioni telematiche preventive.

L'ammissibilità di porre in essere intercettazioni telematiche e/o informatiche allo scopo di prevenire la commissione di delitti di una certa entità, è espressamente prevista dalla più volte citata legge 547/1993 che al suo art. 13 riconosce la possibilità di disporre tali attività anche in relazione alle c.d. *"intercettazioni preventive",* disciplinate dalla L. 7 agosto 1992 n°356, a seguito di una modifica dell'inciso all'art. 25-*ter* di questa legge: *"al comma 1 dell'art. 25-ter del decreto-legge 8 giugno 1992 n°306 convertito, con modificazioni, dalla legge 7agosto 192 n°356, dopo le parole: <<e di altre forme di telecomunicazioni>> sono inserite le seguenti <<ovvero del flusso di comunicazioni relativo a sistemi informatici o telematici>>".* L'evidente finalità, come si evidenziava nel paragrafo 1.2.d), è di assicurare un ampliamento degli strumenti di lotta alla criminalità organizzata, in relazione alla quale lo strumento della prevenzione assume come evidente una valenza di particolare momento[61].

Interamente riscritto dalla l. 15 dicembre 2001, n. 438, di conversione del d.l.18 ottobre 2001, n. 374 *(recante disposizioni urgenti volte al contrasto del terrorismo internazionale)*, l'attuale **art. 226 disp. att. c.p.p.** *(Intercettazioni e controlli preventivi sulle comunicazioni)* abroga ogni precedente prescrizione in materia di intercettazioni preventive. Debbono, pertanto, ritenersi non più vigenti gli artt. 16 l. 13 settembre 1982, n. 646, 1 quinquies comma 7 d.l. 6 settembre 1982, n. 629, convertito in legge 12 ottobre 1982, n. 726, 2 comma 2 quater d.l. 29 ottobre 1991, n. 354, convertito in l. 30 dicembre 1991, n. 410 – dettati in tema di controllo di soggetti sottoposti a

[60] per tutti cfr.: Cass. Sez. I, 7.04.2004, n.19072, Pizzi; Cass. Sez. IV, 01.07.2003, n.226387; Cass. Sez. I, 29.09.2000 n.217548, Bayan; Cass. Sez VI, 30.09.2003, n. 40330, Cirasole; Cass. Sez. Fer. n.35107 del 19.08.2008, Bruno; Cass. Sez. VI, 16.06.2005 n.28514, Contorno; Cass. Sez. V n. 46454 del 22.10.2008, Oldi; Cass. Sez. I, 07.10.2005 n. 45103, Schneeberger; Cass. Sez. VI, 05.10.2005 n. 41203, Ammaturo.

[61] Uguccioni, sub art. 12 L. 547 del 1993, in Legislazione Penale, 1996, 144.

misure di prevenzione. A tal proposito inoltre, merita di essere sottolineato che il citato d.l. n° 374 del 2001, all'art. 3 co. 2, intervenendo direttamente sul testo della l. 356 del 1992 (come modificata dalla l. 547/1993), prevede che all'art. 25 *bis* di detta legge sia aggiunta, (<<*dopo le parole procedura penale*>>) la frase: *"ovvero nei delitti con finalità di terrorismo"*, estendendo espressamente a queste ultime ipotesi - stavolta senza possibilità di fraintendimento, *cfr. supra* il cit. *1.2.d)* - la possibilità di disporre le intercettazioni informatiche.

Si tratta, come è noto, di intercettazioni disposte a prescindere da qualsivoglia controllo di tipo giurisdizionale e, di conseguenza, prive di ogni valore processuale[62].

Anzi, come è stato correttamente osservato, se corrisponde al vero che la modifica in commento scaturisce dall'esigenza di prevenire il compimento di determinati reati – garantendo la disponibilità di dati ed informazioni di sicura rilevanza in vista dello sviluppo delle indagini –, non appena acquisita la notitia criminis, di regola, le intercettazioni preventive devono immediatamente cessare[63].

Peraltro, Il comma 5 dell'**art. 226 disp. att. c.p.p.**, prescrive espressamente che gli elementi acquisiti attraverso le attività preventive non possono essere utilizzati nel procedimento penale. Essi non possono essere menzionati in atti di indagine, né costituire oggetto di deposizione, né essere altrimenti divulgati.

A tal proposito, l'art. 5 comma 3 bis della legge di conversione introduce una nuova figura criminosa, inerente appunto la illecita divulgazione o pubblicazione (anche solo parziale) del contenuto delle suddette captazioni.

Tassativa ancora è l'individuazione della gamma di reati in relazione ai quali l'attività intercettiva *de qua* può essere esperita.

Il riferimento è ai crimini di cui agli **artt. 51 comma 3 bis** e **407 comma 2 lett. a n. 4 c.p.p.** e, dunque, a delitti di particolare allarme sociale, per la prevenzione dei quali il legislatore ha consentito l'ingerenza della pubblica autorità nell'esercizio del diritto al rispetto della vita privata e familiare ex **art. 8 C.e.d.u.**

La richiesta di autorizzazione all'attività di captazione preventiva può essere avanzata dal Ministro dell'interno o, su sua delega, dai responsabili dei servizi centrali, ovvero dal questore, dal comandante provinciale dei Carabinieri e della Guardia di finanza.

Con particolare riferimento ai reati di cui all'art. 51 comma 3 bis c.p.p., la facoltà in parola può essere delegata al direttore della direzione investigativa antimafia.

Legittimato a concedere l'*autorizzazione de qua* è il procuratore della Repubblica presso il capoluogo del distretto in cui si trova il soggetto da controllare ovvero, laddove detto luogo non sia determinabile, del distretto in cui sono emerse le esigenze di prevenzione.

---

[62] Ferma restando la necessità, anche in tali casi, di procedere all'iscrizione delle notizie di reato risultanti dall'attività svolta. In questo senso Parodi, La disciplina delle intercettazioni telematiche, in Criminalità informatica, 2002 pg. 892 e ss.

[63] Garuti, Le intercettazioni preventive nella lotta al terrorismo internazionale, in Dir. pen. proc., 2005, 1427.

Le eventuali proroghe (di venti giorni) sono autorizzate, con decreto motivato, dal PM[64]; il primo termine dell'implementazione è pari a quaranta giorni.
La legge processuale nulla dice circa la forma che il provvedimento di autorizzazione deve rivestire (diversamente da ciò che si ha per le proroghe).
Non di meno, non si dubita in dottrina del fatto che esso debba consistere in un decreto motivato. Ciò, in ossequio a quanto statuito dall'art. 15 comma 2 Cost.[65]
Dell'esito delle intercettazioni è redatto verbale sintetico, depositato, in uno con i supporti utilizzati, nella segreteria del procuratore che ha autorizzato l'attività. Detto deposito deve avvenire nel termine di cinque giorni. Avvenuto il deposito, il procuratore, verificata la conformità delle attività compiute all'autorizzazione, dispone l'immediata distruzione dei supporti e dei verbali. Ai sensi del comma 4, con le modalità e nei casi di cui ai commi 1 e 3, può essere autorizzato il tracciamento delle comunicazioni telefoniche e telematiche, nonché l'acquisizione dei dati esterni relativi alle comunicazioni telefoniche e telematiche intercorse e l'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni[66].
Si rileva infine che nessun particolare significato è da attribuirsi alla differente formula utilizzata dal legislatore nell'art. 13 della L. 23 dicembre 1993, n. 547, rispetto a quella dell'art. 11 (della stessa legge), laddove solo quest'ultima contempla la possibilità (trasfusa nell'art. 266bis c.p.p.) di intercettazione, oltre che del flusso di comunicazioni relativo a sistemi informatici o telematici, anche di quello *"intercorrente tra più sistemi"*. Si tratta verosimilmente di una mera imprecisione legislativa (una delle tante, sic!), alla luce di una valutazione sia teleologica – *se lo strumento dell'intercettazione preventiva risulta in concreto di particolare efficacia nella lotta alla criminalità organizzata, nella sue manifestazioni maggiormente "tecnologiche", nessun senso avrebbe escludere la possibilità di intercettare proprio quelle comunicazioni tra sistemi che verosimilmente possono assumere le connotazioni investigative di maggior rilievo*[67] - che sistematica - alla luce del fatto che l'inutilizzabilità in sede processuale di tutte le intercettazioni preventive non giustifica una limitazione *"garantista"* per atti che, al contrario, possono essere oggetto di decreto di autorizzazione "ordinario" ex art. 266 c.p.p. e come tali "entrare" nel materiale probatorio processuale.

[64] Così dispone il co.2 dell'art. 226 disp. att. c.p.p., non precisando se questi è da individuarsi nel Procuratore ovvero da un sostituto all'uopo designato.

[65] Caprioli, Le disposizioni, cit., 15; FILIPPI, Terrorismo, cit., 167; RUGGERI, Sub art. 5 d.l. 18 ottobre 2001, n. 347, conv. con mod. dalla l. 15 dicembre 2001, n. 438, in Legisl. pen., 2002, 795.

[66] C.d. "Blocco", vale a dire l'operazione volta a registrare gli estremi di un colloquio telefonico (mittente, destinatario, ora, frequenza dei contatti), ma non il suo contenuto. «la comunicazione si svolge nei modi consueti, senza essere interrotta; semplicemente, idonee apparecchiature identificano i soli elementi cui abbiamo accennato». Così Camon in *Le intercettazioni*, cit, 28.

[67] In questo senso Parodi, La disciplina delle intercettazioni telematiche op. cit.

1.4 L'oggetto delle intercettazioni informatiche e telematiche.

1.4.a) Premessa.

Le dimensioni odierne raggiunte dal fenomeno rappresentato dai cd. computer crimes, di pari passo con la diffusione dell'uso di sistemi informatici nella Pubblica Amministrazione e nell'attività imprenditoriale, impongono, oggi più che mai, uno sforzo di produzione normativa e di classificazione delle fattispecie penali che tenga conto del continuo, diuturno, aggiornamento tecnologico che investe la materia.

Il Legislatore Italiano, spesso in adempimento di obblighi di cooperazione europea od internazionale, ha nell'ultimo decennio introdotto nell'ordinamento diverse disposizioni aventi come oggetto la tutela dei "sistemi informatici". A titolo di esempio si possono ricordare:

- L. 547/1993 (modifiche ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica);
- L. 197/1991 (norme per prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio);
- D. L.vo 82/2005 (Codice dell'amministrazione digitale; norme in materia di documentazione informatica e di firma elettronica e digitale)
- L. 248/2000 (modifiche alla legge 633/1941, in tema di diritto d'autore);
- L. 269/1998 (norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, anche condotti per via telematica);
- D. L.vo n. 196 del 30.06.2003 (codice in materia di protezione di dati personali, così come modificato dalla Legge n. 45/2004);
- L. 38/2006 (disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet);
- L. 48/2008 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica);

In nessuna delle norme appena menzionate il Legislatore ha fornito una definizione precisa di "sistema informatico" (indispensabile per l'interprete!), e così, come sovente accade, è stato (come si vedrà *infra*) compito della Giurisprudenza rinvenirne una nozione unitaria che fosse compatibile con le esigenze di tutela, sottesa alla copiosa produzione normativa in materia, dei diversi beni giuridici protetti.

1.4. b) I sistemi informatici.

Rispetto alle comunicazioni informatiche o telematiche, sotto il profilo squisitamente tecnico, possono divenire oggetto di intercettazione tutte le connessioni – fisse od occasionali – *tra sistemi informatici o telematici*, ossia tra computer collegati tra loro in rete o via modem o con qualsiasi altra forma (esistente o "esistenda") di interconnessione. Alla predetta categoria, in base all'orientamento prevalente, possono essere ricondotte, altresì, l'intercettazione delle trasmissioni in

facsimile, delle connessioni cioè via telefax, che avvengono come noto previa demodulazione dei toni mediante le linee telefoniche (trattandosi appunto di comunicazioni tra sistemi telematici).
Diverse del resto, come si accennava nel paragrafo precedente, sono le disposizioni aventi come oggetto la tutela dei "sistemi informatici".
All'art. 1, la Convenzione di Budapest del 2001 fornisce una definizione che potremmo dire iniziale di *"sistema informatico"*, intendendo per esso *"qualsiasi apparecchiatura isolata o un insieme di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati"*.
Tuttavia, in assenza di un'univoca definizione legislativa interna, è stata la giurisprudenza a tentare di fornire una definizione generale di "sistema informatico" e, da questa, di "sistema telematico".
Va tuttavia evidenziato, preliminarmente, come le predette comunicazioni, seppur non intercorrenti direttamente fra esseri umani, sono state assimilate a speciali forme di comunicazioni tra persone dal legislatore del 1993 che, novellando l'art. 623 bis c.p., ha espressamente accomunato tali tipologie di "conversazioni" (e più in generale qualsiasi trasmissione a distanza di immagini, suoni o altri dati) a quelle che viaggiano sulla linea telefonica o telegrafica.
Va segnalato infatti come la peculiarità delle comunicazioni informatiche e telematiche sia costituita non solo dallo strumento di trasmissione, ma soprattutto dalla particolare forma ("digitale" per l'appunto) nella quale si manifestano dati, informazioni, immagini e suoni. Un computer è in effetti un apparato elettronico che funziona per mezzo di appositi programmi, con segnali oggetto di elaborazione digitale denominati bit (intendendosi per byte un insieme di otto unità minime di informazioni, ossia di bit).
L'intercettazione informatica o telematica avrà quindi per oggetto proprio i segnali digitali che non si presentano come immediatamente intellegibili per gli "interlocutori informatici" così come per l'operatore che pone in essere l'intercettazione; segnali che dovranno, ovviamente, essere successivamente resi comprensibili.
La norma prende per di più in considerazione sia le comunicazioni che possono intercorrere all'interno di un sistema informatico sia quelle che possono intervenire tra più sistemi. La legge 23 dicembre 1993 n°547, come si diceva *supra,* non contempla peraltro una definizione di *"sistema"* - definizione d'altra parte indispensabile per l'interprete; volendoci cimentare allora nel difficile compito di definire un sistema di questo tipo, potremmo intendere con detta espressione, nella sua particolare accesione,un elaboratore funzionante in rapporto ad altri elaboratori – o comunque ad apparecchiatura funzionalmente connesse, quali stampanti, scanner, fax – ossia un più o meno complesso articolato di attrezzature o macchinari in grado di interagire tra loro. Di particolare interesse si rivela quindi la possibilità di intercettare un flusso di fax tra vari elaboratori, stante la diffusione dell'utilizzo di tale mezzo nelle attività economiche ed attualmente anche le comunicazioni a mezzo

di posta elettronica, che per molti aspetti hanno sostituito le "ordinarie" comunicazioni telefoniche.

In particolare, quindi, un **sistema informatico** è di regola costituito da più elaboratori collegati tra loro per scambiarsi dati ovvero da ogni macchina elettronica che presenti una connessione organica di elementi funzionale ad uno scopo e che utilizzi un microprocessore per l'elaborazione di dati binari (*bit*), purché sia dotata di propria autonomia, ossia risulti in grado di eseguire le proprie funzioni senza ricorrere all'ausilio di alti sistemi.

Inoltre – circostanza anche questa presa in considerazione dalla norma – più sistemi informatici possono occasionalmente collegarsi tra loro per ottenere informazioni o scambiare e prelevare dati.

Un sistema informatico risulta quindi costituito da più apparati informatici necessariamente collegati tra loro per lo scambio di informazioni e conoscenze, con connessioni di carattere permanente o, quantomeno, non occasionali (ad es. attraverso i canali di comunicazione televisivi, satellitari o telefonici). Anche il singolo elaboratore può, a ben guardare, essere ragionevolmente ricondotto al concetto di sistema informatico, ove si intenda come tale un sistema di risorse composto da dispositivi di elaborazione elettronica digitale, programmi memorizzati e gruppi di dati che, sotto il controllo dei programmi memorizzati, immette, tratta ed emette automaticamente dei dati che può memorizzare e recuperare di modo da rendere anche a quest'ultimo – inteso nella sua globalità funzionale – applicabile la tutela codicistica[68].

Sul tema, la Suprema Corte, in una importante decisione[69], ha riconosciuto la natura di *"sistema informatico"* alla *rete telefonica fissa* sia per le modalità di trasmissione dei flussi di conversazioni sia per l'utilizzazione delle linee per il flusso dei cc.dd. *"dati esterni alle conversazioni"* in un caso in cui erano stati contestati i reati di *"accesso abusivo ad un sistema informatico"* e di *"frode informatica"*. La Suprema Corte, in particolare, ha precisato che deve ritenersi "sistema informatico", secondo la ricorrente espressione utilizzata nella l.547 del 1993 che ha introdotto nel codice penale ipotesi specifiche di reati informatici *<<…un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate – per mezzo di un'attività di "codificazione" e "decodificazione" – dalla "registrazione" o memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati" cioè di rappresentazioni elementari di un fatto, effettuate attraverso simboli (bit), in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni" costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente. La valutazione circa il funzionamento di apparecchiature a mezzo di tali tecnologie costituisce giudizio di fatto insindacabile in cassazione ove sorretto da motivazione adeguata ed immune da errori logici. >>.*

[68] Così Galdieri, *Teoria e pratica nell'interpretazione del reato informatico,* Milano, 1997, 40.

[69] Cass. Sez VI del 14.12.1999 n°214945, Piersanti, in CED Cass. N. 214945

Si tratta di una definizione incentrata, come evidente, sul passaggio dal *"dato"* all' "*informazione*"; nel senso che alla funzione di registrazione - memorizzazione elettronica di dati intesi quali "rappresentazioni elementari di un fatto" si affianca la funzione complementare di elaborazione-organizzazione logica di tali dati in insiemi più o meno estesi costituenti apunto "informazioni".
L'attitudine della macchina (computer) ad organizzare ed elaborare dati sulla base di un certo programma (software) ed in vista di finalità eterogenee, costituisce quindi elemento discretivo essenziale, consentendo di distinguere ciò che è "informatico" da ciò che è invece solamente "elettronico". Così, ad esempio, il videoregistratore, il lettore di CD (sempre che non siano connessi ad un computer con funzione di masterizzazione o elaborazione di immagini e suoni), i dispositivi che presiedono all'attivazione dei sistemi di sicurezza sulle auto (come l'airbag, o l'ABS), certi elettrodomestici a tecnologia digitale sempre più diffusi nelle nostre case, non possono considerarsi – proprio perché inidonei alla elaborazione ed organizzazione di dati nel senso che si è detto – "sistemi informatici", quanto solamente o, se si vuole, più semplicemente, apparati elettronici.

1.4.c) I sistemi telematici.

Per quanto concerne poi, specificatamente, la nozione di *"sistema telematico"*, questa può essere spiegata muovendo dalla definizione di sistema informatico, aggiungendo però taluni elementi ulteriori.
Infatti, più sistemi informatici collegati stabilmente tra loro mediante apparati di comunicazione (per esempio via modem o anche via radio se connessi con tecnologia *wireless*) al fine di permettere la trasmissione a distanza delle informazioni precedentemente elaborate e raccolte, costituiscono un "sistema telematico".
In tal caso l'elemento che consente di ravvisare un sistema "telematico" in luogo di un mero dispositivo di trasmissione a distanza di segnali (come il telefono o il fax) è dato proprio dal fatto che ad essere collegati tra loro sono due (o più) sistemi "informatici": tipico è il caso dei sistemi di posta elettronica o di connessioni tramite terminali remoti (per esempio il bancomat).
Di grande interesse si presenta la definizione che di sistema telematico dà, a Sezioni Unite, la Corte di Cassazione la quale, al fine di sussumere l'apparato di telefonia mobile/cellulare alla nozione di sistema telematico, così argomenta: *<< La moderna telefonia mobile si svolge col sistema cellulare (trasmissione tramite rete di terra) o satellitare (il segnale giunge a destinazione via satellite), ma anche quella fissa si è adeguata alle nuove tecnologie. In particolare, fu introdotto il sistema cellulare di tipo analogico non ancora adatto alla trasmissione di dati (apparecchi AMPS, TACS, ETAX) e che utilizzava la modulazione di frequenza…(omissis…). In concreto - continua la Corte - le linee telefoniche, secondo la moderna tecnologia, attuano la trasmissione delle comunicazioni con la conversione (codificazione) di segnali fonici in forma di "flusso" continuo di cifre, e detti segnali, trasportati all'altro estremo, vengono*

ricostruiti all'origine (decodificazione)…(omissis) . Trattasi, dunque, di flussi relativi ad un sistema tecnico che s'innesta nella disciplina delle intercettazioni di comunicazioni informatiche o telematiche, captate a sorpresa nel corso del loro svolgimento, che hanno per oggetto anche la posta elettronica (e-mail) da computer a computer collegati alla rete internet in forma ibrida per mezzo di SMS da computer (collegato alla detta rete) ad apparecchi cellulari GSM o vice-versa. Il flusso è il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici. Fra strumenti informatici, quindi, è possibile lo scambio di impulsi in cui si traducono le informazioni; scambio che è comunicazione al pari della conversazione telefonica, sicché la relativa captazione nel momento in cui si realizza costituisce intercettazione[70] *>>.*

Dalle due precedenti Massime si deduce agevolmente come l'intero sistema telefonico a disposizione degli utenti - e indirettamente l'intero sistema delle intercettazioni disposte dalla A.G. – si identifichi ormai, pacificamente, in un gigantesco e complesso sistema telematico.

Del resto, le dimensioni odierne raggiunte dal fenomeno rappresentato dai *cd. computer crimes*, di pari passo con la diffusione dell'uso di sistemi informatici nella Pubblica Amministrazione e nell'attività imprenditoriale, impongono, oggi più che mai, uno sforzo di produzione normativa e di classificazione delle fattispecie penali che tenga conto del continuo, diuturno, aggiornamento tecnologico che investe la materia.

Pertanto, deve ritenersi definitivamente "sfumata" la differenza (diremmo) "ontologica" tra comunicazione telefonica e comunicazione telematica; assimilazione quest'ultima che – per ciò che qui maggiormente interessa – non manca di riverberare i propri effetti sulla (tuttora) esistente distinzione codicistica e di disciplina tra intercettazioni telefoniche (dette anche ordinarie) ed intercettazioni telematiche (ex art 266 bis c.p.p.); e ciò ancor di più ove si tenga conto della c.d. tecnologia Voip che sta effettivamente rivoluzionando il mondo della telefonia grazie alla possibilità di instaurare conversazioni vocali (fra l'altro gratuite o a basso costo) tramite internet (su questo aspetto cfr. *infra*).

1.4.d) L'acquisizione dei cc.dd. "tabulati".

A proposito delle intercettazioni telematiche (e della loro obiettiva difficoltà di definizione), una questione non ha mancato di suscitare (a più riprese) vivo interesse. E' quella relativa ai c*c.dd. dati esterni alle conversazioni telefoniche* - documentati in tabulati (ai fini contabili, fiscali, ecc.) dall'ente gestore, concessionario del servizio di telefonia - ed alla loro eventuale acquisizione e successiva utilizzazione, nei procedimenti/processi penali.

[70] Cass. SS.UU. Sent. n.6 del 23.02.2000, D'Amuri.

In base ad una prima risalente sentenza delle Sezioni Unite della Corte di Cassazione, infatti, l'acquisizione dei c.d. dati esterni doveva ritenersi rientrante nel concetto di **intercettazione informatica**, *"poiché la stampa dei tabulati concernenti il flusso informatico relativo ai dati esterni delle comunicazioni telefoniche costituisce la documentazione in forma intelligibile, del flusso medesimo"*, e quindi *"la relativa acquisizione soggiace alla stessa disciplina delle garanzie di segretezza e libertà delle comunicazioni a mezzo di sistemi informatici di cui alla l. 23 dicembre 1993, n. 547..."*[71]. Il portato di tale pronuncia - che d'altronde non riuscì a mutare il contrario orientamento dei giudici di merito - non era però apparentemente conciliabile con il già ricordato insegnamento giurisprudenziale sul requisito della contestualità[72], secondo il quale, affinché vi sia intercettazione, la comunicazione deve essere captata, appunto, mentre è in corso. Per cui una successiva sentenza[73], sempre delle sezioni unite della Corte di Cassazione, ha poi chiarito che *"ai fini dell'acquisizione dei tabulati contenenti i dati esterni identificativi delle comunicazioni telefoniche conservate in archivi informatici dal gestore del servizio è sufficiente il decreto motivato dell'autorità giudiziaria, non essendo necessaria, per il diverso livello di intrusione nella sfera della riservatezza che ne deriva, l'osservanza delle disposizioni relative all'intercettazione di conversazioni o comunicazioni di cui agli artt. 266 e segg. c.p.p."*.

La necessità del decreto del p.m. sarebbe derivata poi - in mancanza di un'espressa disciplina della materia - dall'eterointegrazione dell'art. 256 c.p.p. (sull'acquisizione dei documenti riservati) operata dal citato cpv dell'art. 15 Cost.

Quindi, secondo le Sezioni Unite i cc.dd. dati esterni rappresentano comunque una comunicazione informatica - circostanza, quest'ultima, negata peraltro da autorevole dottrina[74] - ma l'acquisizione dei relativi tabulati non costituisce intercettazione, perché, tramite essa, non vi è *"alcuna intromissione in sistemi informatici, deputati alla trasmissione di comunicazioni, al fine di captarle."*.

In seguito, allorquando - mediante una modifica dell'art. 132 del d.lgs. n. 196/03 (c.d. Codice della privacy) operata, dapprima, dal d.l. n. 354/03 convertito con modifiche dalla l. n. 45/04, e dunque dalla l. n. 155/05 - il legislatore intervenne direttamente a regolamentare la "delicata" questione, optò espressamente per la scelta più rigorista, richiedendo, appunto, ai fini dell'acquisizione dei tabulati, l'emissione del provvedimento del gip. Ma l'opzione, inverò, non mancò di suscitare una certa perplessità: da un lato, perché tra i due diversi fenomeni - intercettazione ed acquisizione dei c.d. dati esterni - residuava comunque una differenza di disciplina processuale, in quanto l'art. 68 co.3 Cost. continuava a prescrivere la necessaria autorizzazione preventiva, da parte della Camera cui i parlamentari appartengono, solo ai fini della sottoposizione degli stessi ad intercettazione e non anche per l'acquisizione dei "tabulati" loro relativi; dall'altro, e più in generale, perché metteva

[71] Cass. pen., Sez. Un., 13 luglio 1998, in Guida al dir., 1998, f.48, 60, con nota di Bricchetti.

[72] Corte cost., 11 marzo 1993, n. 81, in Giur. cost., 1992, 737.

[73] Cass. pen., sez. un., 23 febbraio 2000, in Giur. it., 2001, 1701 ss., con nota di Idda.

[74] Cfr. Idda, op. cit., 1705 ss.

in luce quanto potessero risultare incerti i confini tanto dell'espressione "intercettazione" quanto quella di "comunicazioni informatiche o telematiche", anche in considerazione del comma secondo dell'art. 240 c.p.p. (novellato poco prima), che prendeva in considerazione unitariamente "dati e contenuti" delle comunicazioni e conversazioni.
Orbene, l'attuale assetto della disciplina si deve comunque alle ulteriori modifiche apportate al testo unico sulla privacy dal D.lgs. 30 maggio 2008 n°109; provvedimento, quest'ultimo, emanato in attuazione della Direttiva Comunitaria 2006/24/CE (c.d. Frattini), a fronte della quale gli Stati Membri si sono visti costretti ad imporre ai gestori telefonici specifici limiti temporali per la conservazione dei dati, oltre che un'analitica regolamentazione della tipologia delle informazioni acquisibili che attribuisce, da ultimo, al PM la competenza ad ordinare alle compagnie telefoniche (o agli Internet Providers - su cui si veda *infra*) l' "esibizione" dei cc.dd. tabulati. Il succitato potere è esercitabile mediante emanazione di un decreto motivato[75].

1.4.e) La generazione e conservazione dei dati del traffico telematico. *I cc.dd. file di log*[76]*.*

In tema di generazione e conservazione dei dati del traffico telematico rileva in primo luogo il *profilo soggettivo*, ovvero l'individuazione dei soggetti obbligati alla conservazione dei cc.dd. *file di log*[77] .
La norma individua tali soggetti nei "fornitori" di comunicazione (sostanzialmente gli ISP: Internet *Services Providers*), ma nelle ipotesi speciali di cui ai commi 4 *ter*, *quater* e *quinquies* dell'art.132 del "codice della privacy", recentemente introdotti dalla legge 48/2008 (compresa l'ipotesi di cui all'art.600-ter comma 1 CP), ai "*fornitori"* devono ora aggiungersi gli *"operatori"* di servizi informatici e telematici, rispetto ai

[75] La Cass. Pen Sez. I, sent. n°2532 dell 2008 ha ritenuto che, ai fini dell'acquisizione dei tabulati relativi al traffico telefonico, l'*obbligo di motivazione* del provvedimento acquisitivo, stante il modesto livello di intrusione nella sfera di riservatezza delle persone, può essere soddisfatto anche con espressioni sintetiche, nelle quali si sottolinei la necessità dell'investigazione in relazione alla prosecuzione delle indagini ovvero all'individuazione dei soggetti coinvolti nel reato o si richiamino, con espressioni indicative della loro condivisione da parte dell' A.G., le ragioni esposte dalla Polizia Giudiziaria.

[76] Per un'indispensabile integrazione della nozione di *file di log* cfr. quanto riportato nei para 4.1.f) e ss. *infra*

[77] I *File di log* sono *file* (il termine *file* - in inglese "archivio" - ma comunemente tradotto anche con "documento") che rappresentano un contenitore di informazioni/dati in formato digitale in cui vengono registrate le attività compiute per esempio da un'applicazione, da un server, o da un interprete di comandi. Ad ogni collegamento sul server relativo al sito web visitato, vengono scritte informazioni relative all'accesso dell'utente (*IP address*, data, ora, pagina richiesta, login, account). Profili di analogia, sotto il profilo della "data retention" presentano i *cookies*, che sono brevi stringhe alfanumeriche che il server invia al browser dell'utente quando questi si connette per la prima volta, allo scopo di immagazzinare specifici dati. Successivamente il browser dell'utente invia una copia del cookie al server in occasione di ogni nuova connessione in modo da permettere al provider di ricordare i dati del visitatore.

quali, in assenza di una definizione del termine "operatore" e dovendosi distinguere quest'ultimo dal "fornitore", sembra di capire che ci si riferisca in maniera indiscriminata ai *fornitori di contenuti e di servizi* (per esempio, ai motori di ricerca, ma anche ai contatori, ai broker pubblicitari nel web, e addirittura a tutti i "content provider").

Ma a rilevare è anche il *profilo oggettivo*, ovvero l'indicazione di quali dati generare e conservare, dovendosi considerare assai generica la definizione contenuta nella norma di *"dati relativi al traffico"*. L'unico parametro di riferimento per l'individuazione analitica dei "dati" da generare e conservare è al momento definito, con procedimento *ex adverso,* dai provvedimenti del Garante che ribadiscono il divieto della conservazione di taluni dati (per esempio, il contenuto delle comunicazioni) e che impongono (ancora una volta in modo assai generico) i principi di "pertinenza" e di "non eccedenza", ma tutto ciò non vale a colmare le carenze derivanti dalla mancanza di una definizione di *"dati relativi al traffico"*.

La direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 riguardante *la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, enumera le "categorie di dati da conservare" (art.5), i quali, con riferimento a internet, più precisamente sono:

a. <u>i dati necessari per rintracciare e identificare *la fonte di una comunicazione* per l'accesso Internet, posta elettronica su Internet e telefonia via Internet:</u>

   i) identificativo/i dell'utente;

   ii) identificativo dell'utente e numero telefonico assegnati a ogni comunicazione sulla rete telefonica pubblica;

   iii) nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati assegnati l'indirizzo di protocollo Internet (IP), un identificativo di utente o un numero telefonico;

b. <u>i dati necessari per rintracciare e identificare *la destinazione di una comunicazione* (limitatamente alla telefonia fissa e mobile e alla posta elettronica con esclusione implicita dei dati relativi all'accesso a internet):</u>

c. <u>i dati necessari per determinare la data, l'ora e la durata di una comunicazione:</u>

   data e ora del log-in e del log-off del servizio di accesso Internet sulla base di un determinato fuso orario, unitamente all'indirizzo IP, dinamico o statico, assegnato dal fornitore di accesso Internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato;

d. i dati necessari per determinare il tipo di comunicazione (limitatamente alla telefonia fissa e mobile e alla posta elettronica con esclusione implicita dei dati relativi all'accesso a internet);

e. i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature:
per l'accesso Internet, la posta elettronica su Internet e la telefonia via Internet:
i) numero telefonico chiamante per l'accesso commutato (dial-up access);
ii) *digital subscriber line* (DSL) o un altro identificatore finale di chi è all'origine della comunicazione;

f. i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile:
1) etichetta di ubicazione (Cell ID) all'inizio della comunicazione;
2) dati per identificare l'ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione (Cell ID) nel periodo in cui vengono conservati i dati sulle comunicazioni.

Il comma 2 dell'articolo 5 recita infine: ***"A norma della presente direttiva, non può essere conservato alcun dato relativo al contenuto della comunicazione".***
Il punto sub b. appare assai rilevante ai fini della possibilità concreta di poter conseguire gli scopi della norma, ovvero la repressione dei reati. Tale punto non annovera, infatti, la possibilità di conservare i dati necessari per rintracciare e identificare la destinazione di una comunicazione con riguardo all'accesso a internet, ma limita tale conservazione alla telefonia e alla posta elettronica. Tale esclusione tuttavia è in grado di vanificare le finalità proprie della norma qualora ciascun utente della rete non venga contraddistinto, di tempo in tempo, con un IP univoco; circostanza che non è del resto resa tecnicamente possibile in tutte le ipotesi di c.d. "*IP masquerading*" .
È il caso, assai frequente in Italia, delle reti NAT[78] che presentano una moltitudine di utenti verso l'esterno con un solo IP pubblico. La prassi di non conservare i dai relativi all'IP di destinazione della comunicazione telematica, unita all'assegnazione del medesimo IP pubblico a una moltitudine di utenti, rende tecnicamente vano ogni tentativo di identificazione degli autori di eventuali reati.
Va sottolineato però che il Dlgs 30 maggio 2008 n. 109 ha introdotto l'obbligo per i "fornitori" di *"assicurare la disponibilità e l'effettiva univocità degli indirizzi di protocollo internet"*.
Rileva infine, sempre sul piano oggettivo, l'adozione di tutti gli accorgimenti tecnici utili a garantire una corretta generazione e conservazione dei dati, ma anche l'esigenza di pervenire a una normalizzazione dei diversi formati di generazione dei dati.

[78] Il funzionamento di dette reti verra spiegato nel successivo Cap. IV, *infra.*

1.4.f) segue: l'acquisizione dei dati del traffico telematico.

L'art.132 del codice della privacy impone la conservazione dei dati ***"per finalità di accertamento e repressione dei reati".***

I dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private.

Giova sottolineare che valgono per i *file di log* tutte le considerazioni che vengono svolte in materia di acquisizione probatoria del dato digitale rispetto all'esigenza di ridurre al minimo il rischio di alterazione. Sempre più spesso, d'altronde, alle lacune derivanti dall'esistenza di norme assai generiche si sommano alcune carenze di specializzazione nel mondo forense.

La questione relativa all'acquisizione dei *log* presso l'ISP è priva di significativi riscontri giurisprudenziali. La prassi consolidata è quella di acquisire i dati formulando una richiesta direttamente al fornitore, delegando quest'ultimo a effettuare l'estrazione, la duplicazione e la trasmissione dei dati all'autorità richiedente.

È ancora aperto il dibattito circa la natura di tale atto di acquisizione, e in particolare se esso costituisca un *"accertamento tecnico"* in senso stretto, e inoltre se lo stesso, in quanto tale, sia ripetibile.

Si tratta evidentemente di questioni di particolare rilevanza (si pensi per esempio all'ipotesi della richiesta di un incidente probatorio), le quali possono essere sviscerate soltanto se si è in grado di conoscere nel dettaglio le modalità tecniche di generazione e conservazione dei dati del traffico.

L'esigenza che si pone in tutta la sua urgenza, quindi, è di poter contare su modelli e linee guida condivise nell'ambito della c.d. *computer forensics* (su cui si dirà *infra*), affinché si possa giungere all'adozione di vere e proprie regole tecniche di generazione e conservazione dei dati, utili a garantirne l'immodificabilità e, soprattutto, l'incontrovertibile attendibilità[79].

Si pensi, per esempio, a un delitto informatico commesso nei confronti di un ISP da parte di un suo stesso cliente/abbonato. In quel caso, l'acquisizione dei *log*, nelle modalità consolidatesi nella prassi, sarebbe rivolta direttamente alla parte offesa, in totale assenza di garanzie circa l'integrità dei dati da estrapolare.

Peraltro, l'acquisizione di un *file di log* ha spesso, obbiettivamente, le caratteristiche di un accertamento tecnico non ripetibile, giacché l'elemento è per sua natura soggetto a continua mutazione (viene aggiornato in continuazione dal sistema) ed impone quindi il ricorso ai criteri di cui all'art 360 c.p.p..

E' infine appena il caso di evidenziare che, se vi sono regole che stabiliscono i tempi di conservazione di alcuni tipi di dati, nessuna norma detta regole tecniche specifiche in ordine alle modalità concrete relative a detta conservazione; regole cioè che

[79] Per una trattazione più approfondita di queste problematiche si rimanda ai para. 2.3 e ss*., infra*

garantiscano l'immodificabilità dei dati ad opera dell'amministratore di sistema e la possibilità di ricostruire *ex post* l'attività svolta su tali elementi[80].

[80] Si riporta, per ragioni di completezza il testo integrale dell'**art. 132 Decreto legislativo 30 giugno 2003 n. 196** (Codice in materia di protezione dei dati personali, come modificato dal d.lgs 109/2008):

1. Fermo restando quanto previsto dall'articolo 123, comma 2, *i dati relativi al traffico telefonico*, sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, *i dati relativi al traffico telematico*, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione.

1-bis. I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni.

2. [abrogato]

3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-quater del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante.

4. [abrogato]

4-bis. [abrogato]

4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale. (8)

4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia.

5. Il trattamento dei dati per le finalità di cui al comma 1 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17, volti a garantire che i dati conservati possiedano i medesimi requisiti di qualità, sicurezza e protezione dei dati in rete, nonché a:

Capitolo II: Reati informatici e procedimenti penali.

***

"La persuasione di non trovare un palmo di terra che perdoni ai veri delitti sarebbe un mezzo efficacissimo per prevenirli… "
(Beccaria C.)

2.1 Il "sottosistema"[81].

2.1.a) Le origini del sottosistema.

Come più volte ricordato nel precedente capitolo, il delinearsi di un ordito infra-codicistico finalizzato a contraddistinguere, con caratteri di marcata autonomia, l'accertamento dei reati informatici risale ai primi anni Novanta del secolo scorso, quando, contestualmente all'introduzione dei *computer crimes* nel catalogo degli illeciti racchiusi nel codice penale, il legislatore, come si è visto, ebbe ad inserire nel sistema una prima forma peculiare di raccolta (o, meglio, di ricerca) della prova c.d. digitale: la captazione telematica, contemplata dall'art. 266 bis c.p.p. Da quel momento in poi, è dato assistere ad un susseguirsi di innesti normativi (non sempre peraltro confinati nell'alveo del codice di rito) che portano oggi a circoscrivere un impianto di certo non organico, ma sufficientemente strutturato da poter vantare un'accentuata emancipazione dai binari ordinari del procedimento penale.
Questo progressivo irrobustimento di forme speciali dell'agire processuale, tra l'altro, ha assunto gradualmente i contorni di un vero e proprio *"sottosistema"* non più e non soltanto volto alla ricostruzione processuale degli illeciti informatici, quanto piuttosto distintivo di tutte quelle situazioni in cui, più in generale, la macchina processuale sia costretta a fare i conti con una piattaforma probatoria a matrice digitale. E' il caso ad es. dei processi aventi ad oggetto reati comuni perpetrati avvalendosi dello strumento informatico e, sempre con maggior frequenza, dei giudizi che, pur attinenti a condotte del tutto svincolate da ogni dimensione tecnologica, debbono confrontarsi con prove a carico e a discarico racchiuse all'interno di un elaboratore, di una rete, o comunque attinte da una connotazione di tipo digitale.
Tornando alla parabola storica che da quel primo esperimento normativo ha condotto sino alle più recenti riforme organiche, nel suo dipanarsi si può intravedere un filo conduttore, ossia la rinuncia, quasi integrale,

[81] Sul tema dei sottomodelli processuali e dei micro-sistemi procedurali autonomi, v., per tutti, Amodio, *Il processo penale tra disgregazione e recupero del sistema*, in Indice Penale 2003 pp. 7 e ss.

da parte dei *conditores* a creare nuove fattispecie processuali in favore di un'espansione o di un riadattamento di istituti tradizionali, all'uopo riplasmati sulla cangiante realtà fenomenica. Si tratta di un percorso che trova il proprio paradigma più nitido proprio nella recente legge 18 marzo 2008 n.48[82] che, per l'appunto, si è in larga misura limitata a "sdoppiare" elementi già esistenti nell'ordinamento, affiancando, a titolo di esempio, alla perquisizione locale di antica tradizione, una perquisizione informatica e, parallelamente, alla classica ispezione dei luoghi, un'ispezione informatica.

Le tappe di questo (ideale) percorso legislativo meritano di essere ricordate.

Orbene, i momenti più significativi del percorso che conduce fino all'attuale assetto della disciplina possono essere ricollegati, a partire dal già richiamato intervento del 1993, essenzialmente e convenzionalmente, a tre stagioni riformatrici. *In primo luogo* quella della **legislazione repressiva della pedopornografia *on line,*** collocandosi nella seconda metà degli anni '90 (l. 15.02.1966 n.66, e soprattutto la l. 03.08.1998 n.269), con una appendice dalle ricadute maggiormente "sostanziali", a circa dieci anni di distanza (l. n.38 del 2006), contraddistinta da una germogliazione di metodi investigativi *ad hoc* (siti civetta, attività di contrasto in rete) e da un impulso verso la specializzazione della polizia giudiziaria.

In seconda battuta, il periodo delle **leggi antiterrorismo** successivo all'abbattimento delle torri gemelle, con il suo apparato di disposizioni d'ampliamento dei controlli sulle comunicazioni anche in via preventiva - sulle quali cfr.. *supra* par. 1.3.f) - (l.15 dicembre 2001 n.438 e d.l. 7 luglio 2005 n.144 e l'influsso sul *c.d. codice privacy* (l. 30.06.2003 n.196) soprattutto in materia di *data retention;* questione, quest'ultima, poi oggetto di molteplici modificazioni e aggiustamenti (l. 26 febbraio 2004 n. 45; l. 31 luglio 2005 n. 155; d.lgs. 30 maggio 2008 n. 109) anche in virtù delle sollecitazioni comunitarie in punto di protezione dei dati personali (direttiva 2006/24/CE, c.d Frattini).

Infine*, terza ed ultima fase*, il tentativo (non sempre riuscito) di *sistematizzazione ratione materiae*, lungo il solco tracciato dalla **Convenzione di Budapest del 2001** (emanata nel contesto del Consiglio d'Europa e sfociata nella citata **l. n. 48 del 2008)**: novella essenzialmente diretta ad imprimere una svolta organica al settore tramite, in primo luogo, il rimodellamento di svariate fattispecie penali sostanziali (quali falsità informatiche, delitti contro la sicurezza dei dati e dei sistemi informatici); quindi attraverso il ripensamento delle attività urgenti della P.G. e di alcuni mezzi di ricerca della prova (ispezioni, perquisizioni e sequestri); per finire con l'allargamento dello spettro della responsabilità degli enti ex d.l. 8 giugno 2001 n.231, all'insieme degli illeciti informatici.

È da questo coacervo di normative che occorre, quindi, prendere l'abbrivio al fine di ricomporre in modo del tutto organico e coerente il quadro di riferimento, tenendo peraltro in debita considerazione altresì i provvedimenti eccentrici rispetto ai tre

[82] Un inquadramento generale circa l'intervento legislativo lo si può rinvenire in Picotti, *La ratifica della Convenzione Cyber Crime e nuovi strumento di contrasto contro la criminalità informatica e non solo* in Dir. Dell'Internet, 2008, pp. 247 e ss.

archi di tempo individuati (si pensi alla legge 20 novembre del 2006 n.281, in punto di intercettazioni telematiche illegalmente formate) e, soprattutto, le divaricazioni dai normali *standard* del processo derivanti tanto dalle prassi forensi, tipiche del particolare campo di indagine, quanto dalla accentuata singolarità della criminalità informatica.
Qui, più ancora che in altri ambiti, sono infatti proprio le "*peculiarità oggettive e soggettive dei fatti da accertare"* a modellare il rito *"secondo profili spesso inediti o comunque sensibilmente originali"*[83].

2.1.b) L'accertamento informatico: specificità

Per quanto detto sopra, l'intera disciplina merita di essere esaminata alla luce delle specificità dell'oggetto dell'accertamento, costituito da quelle evidenze informatiche che, con più sembianti, concorrono a comporre la piattaforma probatoria di ogni processo concernente un *c.d. computer crime*. Non vi è dubbio, infatti, che proprio sul rilievo dei profili di volatilità e modificabilità delle stesse, il *corpus normativo* in parola si sia andato modellando in un modo del tutto peculiare, anche grazie ai richiami derivanti dagli esiti di un'elaborazione dottrinale giunta oggi ad affermare che *"il giusto processo deve riconoscere all'imputato il diritto di essere messo a confronto con il dato informatico nel suo aspetto genuino, senza alterazioni",* evidenziando come "*questa sia la trasposizione moderna del diritto a confrontarsi con l'accusatore"*[84] .
Qualche accenno sul punto non apparirà, quindi, superfluo a partire da una riflessione: se è pur vero che le cautele per preservare l'integrità delle *criminal evidence,* sono, in generale, ben conosciute dai processualisti, essendo in parte già applicate ad altri campi, come quello dei materiali genetici, tuttavia la sottolineata natura ontologicamente fragile, volatile e falsificabile del dato digitale chiama in causa un bagaglio più vasto ed incisivo di procedure atte a garantire attendibilità all'accertamento penale; procedure che – ed è questo l'aspetto di maggiore complessità – debbono interagire con le norme codicistiche. Ecco perché su questo terreno appaiono così centrali questioni quali **"la continuità probatoria"**, vale a dire la tracciabilità del procedimento di repertamento e analisi *"in ogni suo punto mediante la produzione di report a vari livello di dettaglio"*[85] e la cristallizzazione del quadro informatico mediante forme di copiatura e clonazione nell'ottica di un insieme trasparente e verificabile dalle altre parti processuali.
Un ulteriore aspetto che merita di essere considerato, quale coordinata del muoversi tra le pieghe del processo penale per i reati informatici, attiene alla constatazione di come la ricerca della prova digitale incida profondamente sui valori catalogati dalla

[83] Così Amodio, *I reati economici nel prisma dell'accertamento processuale*, in Riv. It di diritto e preoc pen, 2008, 1499
[84] Tonini, *Documento informatico e giusto processo*, in Dir. Pen e Processo 2009 pp. 406 e ss.
[85] Mattiucci - Ddelfinis, *Forensic Computing*, in Rassegna dell'Arma dei Carabinieri, 2006 pp.66 e ss.

nostra Carta Costituzionale, specie oggi che il computer è divenuto, nelle sue varie declinazioni, il centro motore per la gestione dei propri interessi, il principale contenitore dei frammenti di vita e dei dati sensibili di ciascuno; la memoria sempre più estesa di attività e addirittura di spostamenti fisici, oltre che un veicolo essenziale per la comunicazione e l'interazione col prossimo. Le correlate metodologie di indagine, allora, esigono ambiti di ristretta operatività per evitare connotazioni di sproporzionata afflittività e di pregiudizio a beni costituzionalmente protetti[86]. Ciò è ancor più vero ove si ponga mente alle caratteristiche dell'accertamento informatico, spesso condotto – per così dire – a "banda larga", vista la difficoltà di individuare, dalle semplici tracce elettroniche del reato, il soggetto resosi responsabile dell'illecito, la persona, per dirla con parole semplici, che si trovava davanti l'elaboratore nell'istante temporale rilevante ai fini delle indagini. L'inchiesta per i reati a matrice telematica, in effetti, sembra molte volte richiamare, nelle sue scansioni temporali, l'antica distinzione tra prova dell' "ingegnere", relativa all'avvenimento del delitto nella sua consistenza storica ed obiettiva, e prova "specifica", attinente alla ricerca e alla individuazione dell'autore del reato, dal momento che attraverso l'apprensione e l'elaborazione dei dati digitali si possono ricostruire con precisione le modalità di una certa condotta, ma assai più difficilmente l'autore fisico della stessa, ora per la frequente mancanza di elementi di natura non presuntiva circa l'identità del fruitore del dispositivo, ora per la facilità con cui, nell'universo digitale, è possibile fabbricare credenziali artificiose o manipolare il contesto entro cui si è mosso l'agente. Appare allora chiaro come, nella stragrande maggioranza dei casi, le *investigazioni de quibus* finiscano, non sempre legittimamente, con l'allargarsi a dismisura ben oltre il ristretto sentiero del fatto contestato, tanto da far ritenere condivisibili quegli sforzi dottrinali volti ad immaginare, al termine della fase preliminare, possibili udienze di stralcio *"per passare al setaccio le informazioni collazionate e conservare soltanto quelle rilevanti ai fini dell'accertamento"*[87].

Infine, altro fattore da tenere in debito conto - e che complica recisamente l'accertamento informatico - è senz'altro quello della transnazionalità delle indagini in materia, quasi mai caratterizzate da un mosaico probatorio ristretto nei confini nazionali, considerata la generale extraterritorialità (se non vera e propria a-territorialità) del fenomeno internet; il frequente utilizzo da parte degli autori del reato informatico (e non solo) di server ed apparati esteri; il flusso di dati intercorrenti fra più nazioni e l'impiego costante e strumentale (soprattutto da parte dei *crackers* – sui quali si riveda la nota n.36) di c.d. "teste di ponte" estere utilizzate per sferrare, in modalità mascherata, i propri attacchi.

[86] Negli stessi termini in ambito statunitense, Silbert – Chilton, *Gigabit by Gigabit: Technology's potential erosion of the fourth Amendment,* in Crim. Just. 2010, 5

[87] Carnevale, in *Copia e restituzione dei documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in Dir. Pen. e Processo 2009 pp. 481 e ss.

2.1.c) Le attribuzioni del P.M. distrettuale.

Atteso che le intercettazioni informatiche e telematiche sono strumenti di ricerca della prova destinati ad intervenire in ausilio dell'attività degli investigatori prevalentemente (ma, come più volte ribadito, non esclusivamente) nell'ambito dei *computer crimes* - sussistendo fra gli stessi, diciamo, una sorta di corrispondenza "ontologica" - è d'uopo, in questo senso, prendere in considerazioni talune peculiarità procedurali (che contribuiscono ad alimentare, arricchendola, la concezione del sottosistema cui al parag. 2.1.a)) che afferiscono all'ufficio del P.M. che - in concreto - sarà chiamato o a disporre (in via d'urgenza) un'attività di captazione del flusso informatico e/o telematico nell'ambito di un'indagine del predetto tipo, ovvero a richiedere un provvedimento *ad hoc* al giudice competente[88].
Uno degli aspetti maggiormente caratterizzanti le indagini in materia di *Cyber-crimes*, infatti, è sicuramente rappresentato dalla speciale investitura che l'art.51 c.p.p. – così come modificato dalla L. n°48 del 2008, attuativa della Convenzione di Budapest - conferisce al P.M. distrettuale. E' di tutta evidenza come la precedente novella abbia introdotto un'ulteriore eccezione all'ordinaria simmetria tra le regole codicistiche che governano la competenza territoriale del giudice ed i normali criteri di assegnazione delle funzioni al P.M. (in aggiunta a quelle già previste in tema di criminalità organizzata e/o terroristica).
Le investigazioni sui cc.dd. computer crimes, così come quelle a contrasto della pedo-pornografia *on line*, sono dunque oggi devolute all'ufficio del P.M. del capoluogo del distretto di Corte d'Appello nell'ambito del quale ha sede l'organo giudicante territorialmente competente.
E chiara la *ratio* che sottende il predetto "spostamento" che intenderebbe, al pari di quanto si è registrato in tema di criminalità organizzata, garantire una maggiore concentrazione ed un più accurato coordinamento delle relative indagini, sollecitando, nei fatti, la creazione di vere e proprie "Procure Distrettuale Informatiche"[89].
In realtà, ciò ha determinato (frustrando in un certo senso i buoni propositi del legislatore) una gran congerie di disfunzioni oltre che pericolosi ingolfamenti, incidendo negativamente sulla efficacia dell'accertamento e, di conseguenza, sul doveroso rispetto del principio della obbligatorietà dell'esercizio della azione penale (art. 12 Cost.).

---

[88] Per una rassegna degli scritti sullo specifico argomento si rinvia a Cajani, *Considerazioni sull'impatto della "distrettualizzazione"ex legge 48/2008 sul pool reati informatici della Procura di Milano*, in AA.VV., (a cura di Costabile, Attanasio), *IISFA Memberbook 2100 Digital Forensics*, Forlì, 2010, pp. 1 e ss.; Luparia, *Computer crimes e procedimento penale,* in *Trattato di procedura penale,* VII, I (a cura di G. GARUTI), Torino, 2011, p. 377, Cassibba, *L'ampliamento delle attribuzioni del pubblico ministero distrettuale in Luparia (a cura di) Sistema penale e criminalità informatica;* Melillo, *Attribuzioni processuali in tema di misure preventive e di reati informatici* in Mazza, Viganò (a cura di) Misure urgenti in tema di sicurezza pubblica, Torino 2008, 221;

[89] Diddi*, Ritocchi ad attribuzioni e competenze distrettuali*, in Scalfati (a cura di) Il decreto sicurezza, Torino, 2008, 147.

Tra l'altro, se le preesistenti deroghe ai criteri di devoluzione delle funzioni di P.M. trovavano ragion d'essere nell'unità dei fenomeni criminosi da contrastare (mafioso e terroristico, appunto) - generalmente connotati da una estesa articolazione su tutto il territorio nazionale o addirittura sovranazionale - nell'ipotesi in esame, a venire in rilievo sarebbe, al limite, la sola natura specialistica delle indagini riguardanti i reati a matrice tecnologica.

Cionondimeno, esiste un'ulteriore ragione alla luce della quale la (qui criticata) scelta del legislatore appare ancor meno convincente.

Le intercettazioni informatiche e telematiche, com'è noto, quali peculiari strumenti di ricerca della prova possono essere richieste alla A.G. dalla autorità inquirente anche con riguardo a reati che esulano dal catalogo tassativo riportato dall'art.266 c.p.p. presentando, quindi, una sfera di operatività sensibilmente più estesa rispetto alle cc.dd. intercettazioni ordinarie. In altri termini, volendo ulteriormente enfatizzare quest'ultimo concetto, nel caso in cui sussistano le condizioni per disporre una intercettazione telefonica, risulterà sempre possibile procedere anche alla captazione telematica, mentre, viceversa è possibile che, per determinati illeciti informatici di gravità poco meno che bagatellare (si pensi, ad es., ad una querela per un accertato malfunzionamento di una casella di posta elettronica!) possa essere concedibile esclusivamente l'intercettazione telematica, ma non quella telefonica. Si tratta, com'è evidente, di una circostanza non priva di rilievo per la prassi investigativa, ove si consideri che gli organi inquirenti istituzionalmente deputati a perseguire i fenomeni criminali di maggior gravità e pericolosità (mafie e terrorismo)[90] siano chiamati dal legislatore a doversi occupare, al contempo, di eventi criminali di minore entità.

A prescindere dall'esiguità di (valide) motivazioni di politica criminale a supporto di un simile scostamento dal canone generale del giudice naturale (potenzialmente espandibile, ragionando nei medesimi termini, a tutti gli ambiti di indagine connotati da elevata specializzazione), va rivelato come la descritta distonia sistematica risaltava sicuramente ancor di più agli occhi prima che il legislatore non intervenisse ad affidare (con la L.n°125 del 2008 di modifica degli artt. 51 co.3 quinquies e 328 c.p.p.) le correlative funzioni di G.I.P. e di G.U.P. al giudice del capoluogo del distretto (così come del resto avviene anche in tema di criminalità organizzata e terrorismo), mitigando, al contempo, l'eccessiva rigidità nel riparto delle funzioni di P.M. e prevedendo che l'esercizio dell'accusa in dibattimento possa essere altresì affidato ad un sostituto designato dal Procuratore della Repubblica presso il giudice territorialmente competente (ferma restando, tuttavia, la competenza esclusiva a compiere le indagini preliminari in capo al P.M. del capoluogo).

[90] I cui appartenenti spesso - proprio al fine di garantire continuità e maggiore incisività all'azione di contrasto ai fenomeni criminosi che destano maggiore allarme sociale - vengono sollevati da incombenze di carattere organizzativo nell'ambito dell'ordinaria attività di Procura quali, ad esempio, turni per la celebrazione di riti direttissimi, reperibilità notturna etc.

2.1.d) "*locus commissi delicti*" nei reati informatici*:* la teoria dell'*ubiquità.*

Le precedenti considerazioni in tema di competenze specifiche richieste in capo all'ufficio di Procura chiamato in concreto a svolgere indagini, più o meno complesse, in materia di *cybercrimes* (o comunque di reati posti in essere attraverso l'utilizzo di apparati informatici/telematici) trovano puntuale rispondenza nelle difficoltà che caratterizzano le investigazioni preordinate ad accertare il luogo esatto di perpetrazione del c.d. reato "informatico"[91]. Questione quest'ultima assai disputata sia in dottrina sia in giurisprudenza e che accentua ulteriormente il connotato di "sottosistema" (inteso come irrobustimento di forme speciali di carattere tanto sostanziale quanto processuale) che si vuol riconoscere al complesse delle problematiche - di rito, ma appunto, anche sostanziali – connesse alle investigazioni che abbiano ad oggetto crimini informatici.

L'illecito penale informatico infatti (come già accennato e come si vedrà meglio *infra*) è ontologicamente caratterizzato da un elevato tasso di "*internazionalità*" (ma anche, come pure è stato sostenuto, di apolidia), che ne rende sovente davvero difficoltoso l'accertamento.

In quasi tutti i casi è d'altra parte necessario, prima di avviare l'indagine, procedere alla valutazione della sussistenza della giurisdizione dell'autorità giudiziaria italiana sul fatto per cui si procede; sovente, poi, anche laddove la prima verifica sortisca esito positivo, occorrerà procedere ad attività di ricerca e di acquisizione di prove all'estero.

Come noto, le regole di attribuzione della giurisdizione italiana sono contenute negli artt. 6-10 c.p.: in base all'art 6 c.p. è prevista la punibilità secondo la legge italiana di chiunque commette un reato nel territorio dello Stato: ciò avviene ogni qual volta *"l'azione o l'omissione che lo costituisce è ivi avvenuta in tutto o in parte , ovvero si è verificato l'evento che è la conseguenza dell'azione od omissione*".

Il legislatore ha quindi fatto propria la cd. teoria dell' *"ubiquità"*: la norma fa infatti riferimento ad un momento qualsiasi dell'iter criminoso che, considerato unitariamente rispetto successivi atti commessi all'estero, integri un'ipotesi di delitto tentato o consumato. Ne consegue che basterà che anche un frammento della condotta delittuosa si sia verificato in Italia per radicare la potestà punitiva dello Stato.

Il raggio di estensione della giurisdizione italiana (come si dirà più diffusamente *infra*) risulta poi ulteriormente ampliato in tema di delitti contro la prostituzione e la pornografia minorile, e contro la libertà sessuale: ai sensi dell'art. 604 c.p. (modificato dalla L. 7/2006), infatti, i fatti inquadrabili nelle citate fattispecie di reato sono punibili secondo la legge italiana anche quando il fatto è commesso all'estero da cittadino italiano, ovvero in danno di cittadino italiano, ovvero da uno straniero in concorso con un cittadino italiano.

[91] Problematica non secondaria visto che ad essa (fra le tante altre molteplici implicazioni) si riconnette – chiudendo in un certo senso il cerchio - anche l'individuazione del pm competente ad indagare su un dato reato.

Così, facendo applicazione dell'ampia formulazione dell'art. 6 c.p., un accesso abusivo ad un sistema informatico o telematico (ex art. 615-ter c.p.) si potrà considerare ad esempio consumato non solo nel luogo in cui ha sede la banca dati del sito violato, ma anche là dove ha avuto luogo l'evento-accesso al sistema. L' "azione", nel senso voluto dalla norma, in altre parole, coinciderà tanto con l'inserimento delle informazioni necessarie a violare il sistema (in ipotesi, servendosi di una macchina collocata in territorio italiano), quanto con la violazione dei sistemi di protezione del sistema medesimo (in ipotesi, collocato all'estero).
Allo stesso modo, un'ingiuria od una diffamazione immessa in rete o con una comunicazione via e-mail si potrà ritenere consumata non solo nel luogo ove la stessa di fatto viene percepita dalla persona offesa, ma anche - ai fini della giurisdizione - nel luogo in cui l'operatore l'ha immessa in rete.
Di questi criteri ha fatto ampia applicazione la Corte di Cassazione ad esempio in tema di diffamazione a mezzo Internet con la sentenza n. 4741 del 27.12.2000[92].

2.1.e) segue: "*locus commissi delicti*" e i reati di pedo-pornografia a mezzo internet.

Questa soluzione interpretativa è rimasta sostanzialmente immutata nel tempo, pur con gli inevitabili "aggiustamenti" ed "adattamenti" dovuti ai sempre nuovi sistemi di comunicazione elettronica e telematica oggi disponibili (si pensi ad esempio al *file sharing peer-to-peer*) od alla complessità degli schemi relazionali sottesi alla commissione di delitti con il mezzo informatico.

---

[92] *"(omissis)…la possibilità di dare applicazione alla legge penale italiana dipende essenzialmente dalla concreta formulazione delle singole norme incriminatrici, strutturate, di volta in volta, come reati commissivi od omissivi, di danno o di pericolo, di pura condotta o di evento, ecc.. La diffamazione…è un reato di evento, inteso quest'ultimo come avvenimento esterno all'agente e causalmente collegato al comportamento di costui. Si tratta di evento non fisico, ma per così dire, psicologico, consistente nella percezione da parte del terzo (rectius dei terzi) della espressione offensiva…(omissis)…in realtà la percezione è atto non certamente ascrivibile all'agente, ma a soggetto diverso, anche se - senza dubbio - essa è conseguenza dell'operato dell'agente. Il reato, dunque, si consuma non al momento della diffusione del messaggio offensivo, ma al momento della percezione dello stesso da parte di soggetti che siano "terzi" rispetto all'agente ed alla persona offesa….(omissis). Per di più, nel caso in cui l'offesa venga arrecata tramite internet, l'evento appare temporalmente, oltre che concettualmente, ben differenziato dalla condotta. Ed invero, in un primo momento, si avrà l'inserimento "in rete", da parte dell'agente, degli scritti offensivi e/o delle immagini denigratorie, e, solo in un secondo momento (a distanza di secondi, minuti, ore, giorni ecc.), i terzi, connettendosi con il "sito" e percependo il messaggio, consentiranno la verificazione dell'evento. Tanto ciò è vero che nel caso in esame sono ben immaginabili sia il tentativo (l'evento non si verifica perché, in ipotesi, per una qualsiasi ragione, nessuno "visita" quel "sito"), sia il reato impossibile (l'azione è inidonea, perché, ad esempio, l'agente fa uso di uno strumento difettoso, che solo apparentemente gli consente l'accesso ad uno spazio web, mentre in realtà il suo messaggio non è mai stato immesso" in rete"). Orbene, l'art. 6 C.P., al comma secondo, stabilisce che il reato si considera commesso nel territorio dello Stato, quando su di esso si sia verificato, in tutto, ma anche in parte, l'azione o l'omissione, ovvero l'evento che ne sia conseguenza. La c.d. teoria della "ubiquità", dunque, consente al giudice italiano di conoscere del fatto-reato, tanto nel caso in cui sul territorio nazionale si sia verificata la condotta, quanto in quello in cui su di esso si sia verificato l'evento. Pertanto, nel caso di un iter criminis iniziato all'estero e conclusosi (con l'evento) nel nostro paese, sussiste la potestà punitiva dello Stato italiano."*

Così in materia di divulgazione di materiale pedo-pornografico[93], il dettato normativo richiede per tutte le ipotesi enunciate nel citato art. 600 ter c.p., comma 3, la diffusione o divulgazione del materiale pornografico sicché, per la configurabilità del reato, non basta la cessione a singoli soggetti, ma occorre che l'agente propaghi il materiale interessando un numero indeterminato di persone; in un caso su cui ebbe a pronunciarsi la Corte di Cassazione, era stata attivata un'apposita cartella denominata "Pamela" dove l'indagato collocava il materiale pedo-pornografico che condivideva con tutti gli utenti che potevano accedere a quella cartella tramite un software condiviso denominato C6.

Il problema che si pone rispetto ai reati innanzi indicati consiste nell'individuare il confine esistente tra la condotta di divulgazione, diffusione e pubblicazione di materiale pedo-pornografico prevista dall'art. 600 ter c.p., comma 3, e quella di mera cessione del suddetto materiale prevista dal quarto comma del citato articolo. Generalmente i pedofili si servono di siti internet accessibili a chiunque conosca l'indirizzo elettronico di quel sito. Di conseguenza, colui che intende pubblicizzare il proprio materiale pedo-pornografico o stabilire un contatto con il mercato dei medesimi o comunque diffonderlo nella rete si serve solitamente di un sito web in grado, potenzialmente, di raggiungere una serie indeterminata di persone in casi del genere l'inserimento in siti web di foto o video pedo-pornografici integra gli estremi del reato di divulgazione a mezzo internet. Più arduo è il compito del giudice allorché il trasferimento di una foto o di un video pedopornografico avvenga attraverso una chat-line (sistema di comunicazione in tempo reale che permette agli utenti di scambiarsi messaggi e altre informazioni in formato digitale, e che è strutturato come uno spazio virtuale, suddiviso in tante stanze (canali) in cui diversi soggetti possono dialogare). Invero, se da un lato dietro un nick-name si può celare un unico *cyber* navigatore, dall'altro è pur sempre vero che spesso dietro lo scudo elettronico si celano una molteplicità di persone che, se in possesso di *username* e *password*, possono accedere alla *chat line* e quindi farsi trasmettere o trasmettere materiale pedo-pornografico. In casi del genere non si può ignorare l'ipotesi in cui l'apparente trasferimento da stazione a stazione di materiale pornografico infantile copra in realtà un preciso intento di non volere pubblicare su un sito web il materiale stesso, ma di volere ugualmente comunicarlo a molteplici destinatari che, conoscendo l'indirizzo e-mail comunicante ed il nickame del *cyber* navigatore ricevente, possono direttamente ottenere l'invio del materiale vietato. Tale ipotesi, volta a celare una

[93] Cass. Sez. 3, Sentenza n. 593 del 07/12/2006*: "Commette il delitto di divulgazione via internet di materiale pedo-pornografico previsto dal comma terzo dell'art. 600 ter cod. pen. e non quello di mera cessione dello stesso, prevista al comma quarto del medesimo articolo, non solo chi utilizzi programmi di "file-sharing peer to peer", ma anche chi impieghi una "chat line", spazio virtuale strutturato in canali, nella quale un solo "nickname", necessario ad accedere alla cartella-immagini o video, venga utilizzato da più persone alle quali siano state rese note l'"username" e la "password", le quali possono in tal modo ricevere e trasmettere materiale pedo-pornografico; tale sistema rende possibile trasferire il materiale pedo-pornografico a molteplici destinatari e non si differenzia perciò dalla divulgazione vera e propria, sempre che risulti provata in capo all'agente la volontà alla divulgazione, come nel caso in cui la trasmissione sia stata reiteratamente rivolta a più persone"[.....]. "…il prevenuto aveva ammesso di avere utilizzato il software peer to peer per procurarsi e diffondere materiale pedo-pornografico…"*

vera e propria attività divulgativa, non si differenzia dall'attività di divulgazione effettuata apertamente attraverso un sito accessibile a tutti e ciò perché, a condizione che si provi la volontà dell'agente di volere divulgare materiale pornografico infantile, la comunicazione singola ove reiterata a più persone integra gli estremi della condotta divulgativa prevista dal comma terzo dell'articolo 600 ter c.p. Ugualmente, allorché dietro il paravento della singola stazione ricevente si nascondano più persone che, in possesso di *username* e *password*, possono visitare le pagine in uso all'indirizzo, il singolo trasferimento di immagini pedo-pornografiche può assumere un valore indiziante di una vera e propria divulgazione via internet. Trattasi, ovviamente, di valutazione da effettuare caso per caso da parte del giudice del merito. In definitiva, anche la cessione di fotografie pornografiche minorili attraverso una chat-line può configurare il reato ipotizzato (divulgazione quindi e non la meno grave cessione).

2.1.f) Segue: *locus commissi delicti*. I reati posti in essere attraverso internet dalle associazioni criminali.

Altrettanto complicata (ed oggetto di soluzioni divergenti in Giurisprudenza) è l'individuazione del *locus commissi delicti* allorché si sia in presenza di un' associazione per delinquere finalizzata alla perpetrazione di reati attraverso l'utilizzo di applicativi che sfruttano le potenzialità offerte della rete internet. Come illustrato *supra,* la competenza territoriale in ordine al reato di associazione per delinquere si radica nel luogo in cui ne ha avuto inizio la consumazione ai sensi dell'art. 8, comma 3^ del cod. proc. pen. - per tale dovendosi intendere il luogo di costituzione del sodalizio criminoso a prescindere dalla localizzazione dei reati fine eventualmente realizzati[94]. In altre parole, di regola, anche al gruppo criminale costituito per compiere reati sfruttando le molteplici possibilità offerte dalle tecnologie afferenti al mondo di internet, si applicano le ordinarie disposizioni in tema di individuazione del *locus commissi delicti.* Pertanto, qualora tale luogo non sia determinabile in base agli atti processuali, sarà necessario fare riferimento ai criteri suppletivi di cui all'art. 9 cod. proc. pen.[95]. Alla luce del quale, ove non siano comunque percepibili neppure elementi presuntivi che valgano a radicare la competenza territoriale nel luogo in cui il sodalizio criminoso operante su (o per il tramite di) internet si manifesti per la prima volta all'esterno, possono utilizzarsi criteri desumibili dai reati fine, con particolare riferimento a quello della consumazione dell'ultimo reato fine,

[94] Così Cass. Sez. 1^, 24 aprile 2001, D'Urso.

[95] Nella specie, in relazione ad un'associazione criminale costituitasi in internet ed operante concretamente in Italia, Svizzera e Montenegro, avente lo scopo di introdurre in Italia tabacchi lavorati esteri di contrabbando per mezzo di motoscafi che effettuavano sbarchi su tutto il litorale pugliese, nell'impossibilità di individuare il luogo indicato dall'art. 8, comma terzo, c.p.p. e quelli di cui all'art. 9, nn. 1 e 2, dello stesso codice, si è ritenuto corretta l'attribuzione di competenza all'autorità giudiziaria di Bari, operata dai giudici di merito, rispetto a quella di Brindisi, essendo stata iscritta la notizia di reato per la prima volta nel registro di cui all'art. 335 c.p.p. presso la Procura della Repubblica di Bari. *Cass. Sez. 6^, 16 maggio 2000, Lorizzo.*

specialmente nel caso in cui detti reati siano stati tutti commessi nello stesso luogo e siano tutti dello stesso tipo[96].

In altri termini, secondo la giurisprudenza della Suprema Corte, la competenza territoriale a conoscere di un reato associativo "cibernetico" si radica nel luogo in cui la struttura criminosa destinata ad agire nel tempo diventa concretamente operante, a nulla rilevando il luogo di consumazione dei singoli reati oggetto del "pactum sceleris". In difetto di elementi storicamente certi in ordine alla genesi del vincolo associativo, soccorreranno i criteri presuntivi che valgono a radicare la competenza territoriale nel luogo in cui il sodalizio criminoso si è manifestato per la prima volta all'esterno, ovvero in cui si concretino i primi segni della sua operatività.

E in effetti la costituzione di un'associazione per delinquere - anche quando ciò avviene sul WEB - non si verifica per ciò solo nel momento in cui interviene l'accordo fra i compartecipi, ma in quello (solitamente successivo) della costituzione di un'organizzazione permanente, frutto del concerto, anch'esso a carattere permanente, di intenti e di azione fra gli associati. Solo in tale momento infatti - divenendo operante la struttura permanente e presentandosi quel pericolo della commissione dell'attività stigmatizzata dalla legge, che giustifica le singole incriminazioni - si realizza quel minimum di mantenimento della situazione antigiuridica necessaria alla sussistenza dei delitti di costituzione di associazione per delinquere, che segna il momento di perfezione e nel contempo di inizio della consumazione di essi, rilevante ai fini della determinazione della competenza per territorio.

Quindi anche per ciò che riguarda le associazioni criminali che si costituiscono ovvero operano in internet si può, in definitiva, concordare con quella pronuncia - davvero lungimirante - alla stregua della quale se *"difetta la prova relativa al luogo e al momento esatto della costituzione della associazione, soccorre allora il criterio sussidiario e presuntivo del luogo del primo reato commesso o, comunque, del primo atto diretto a commettere i delitti programmati. Ove non sia possibile ancora determinare la competenza per territorio secondo le regole innanzi descritte, è decisivo allora il luogo ove fu eseguito l'arresto, emesso un mandato o decreto di citazione ovvero il luogo in cui fu compiuto il primo atto del procedimento"*[97].

Sotto il profilo in esame, assai interessante si presenta, infine, una (tutto sommato) recente sentenza della Suprema Corte che ha cercato di ricostruire, in via interpretativa, un'inedita fattispecie di sfruttamento della prostituzione online ad opera di un insolito sodalizio criminale composto da provider, fornitori di servizi, gestori di pagine WEB etc. etc. individuandone, al contempo, il locus commissi delicti.

Si tratta della Sentenza n. 15158 del 21/03/2006 che in un suo passaggio particolarmente interessante, testualmente statuisce: *"Le prestazioni sessuali eseguite in videoconferenza via web-chat, in modo da consentire al fruitore delle stesse di interagire in via diretta ed immediata con chi esegue la prestazione, con la possibilità di richiedere il compimento di determinati atti sessuali, assume il valore di*

[96] Cass .Sez. 6^, 4 ottobre 1999, Piersanti.

[97] Cass. Sez. 1^, 7 febbraio 1991, Mulas.

prostituzione e rende configurabile il reato di sfruttamento della prostituzione nei confronti di coloro che abbiano reclutato gli esecutori delle prestazioni o che abbiano reso possibile i collegamenti via internet, atteso che l'attività di prostituzione può consistere anche nel compimento di atti sessuali di qualsiasi natura eseguiti su se stesso in presenza di colui che, pagando un compenso, ha richiesto una determinata prestazione al fine di soddisfare la propria libido, senza che avvenga alcun contatto fisico fra le parti".

Anche quest'ultima assai singolare ipotesi è sintomatica - a prescindere dalle molteplici considerazioni di ordine sostanziale che pur si potrebbero formulare - del carattere di "sottosistema" che deve effettivamente attribuirsi a tutti i diversi fenomeni afferenti alla criminalità informatica ed alle connesse tecniche investigative.

2.2. I *"cybercrimes[98]".*

[98] La materia dei reati informatici è stata ampiamente trattata in dottrina, tra i molteplici contributi dai quali si è preso spunto per l'elaborazione dei paragrafi successivi, si possono indicativamente ricordare: Sieber, *La tutela penale dell'informazione*, in Riv. trim. dir. pen. ec., 1991, (2-3), p. 495 ss.; Piga, *Diritto penale delle tecnologie informatiche*, Torino, 1999; Sarzana di S. Ippolito, Informatica e diritto penale, Milano, 1994; Pecorella, *Il diritto penale dell'informatica*, Cedam, Padova, 2000; Destito – Dezzani – Santoriello, *Il diritto penale delle nuove tecnologie,* in La biblioteca del penalista, collana (diretta da Cerqua), Cedam, Padova, 2007; D'Aiuto – Levita, *I reati informatici: Disciplina sostanziale e questioni processuali*, Giuffrè, Milano, 2012; Cuomo – Razzante, *La nuova disciplina dei reati informatici*, Giappichelli, Torino, 2009; Luparia – Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2009; Amore – Stanca – Staro, *I reati informatici*, Halley editrici (MC), 2010; Picotti, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in Riv. trim. dir. pen. ec., 4, 2011, 827 e ss.; Luparia, *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Giuffrè, Milano, 2012; Flor, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet,* Verona, 2012; Cajani - Costabile - Mazzaraco, *Phishing e furto d'identità digitale. indagini informatiche e sicurezza bancaria*, Giuffrè, 2008; Lisi - Murano - Nuzzolo, *I reati informatici. La Disciplina penale nella società dell'informazione. Profili procedurali*, Maggioli, 2004; Piccinni - Vaciago, *Computer crimes. Casi pratici e metodologie investigative dei reati informatici*, Moretti & Vitali, 2008; Galdieri, *"Reati informatici e responsabilità delle persone giuridiche: l'Europa chiede una riforma – Reati informatici e attività di indagine - Lo stato dell'arte e prospettive di riforma", 2006;* Aterno, *Le fattispecie di danneggiamento informatico*, in Luparia (a cura di), Sistema penale e criminalità informatica, Milano, 2009, p. 35 ss.; Costabile, *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008*, in Ciberspazio e diritto, 2010, (3), p. 465 ss; Di maria -Mignone, *I "cybercriminali": rischi e limiti dei profili criminologici,* in Ciberspazio e diritto, 2001, (2), p. 3 ss.; Flor, *Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto,* in Dir. pen. proc., 2008, (1), p. 106 ss.; Giannantonio, *L'oggetto giuridico dei reati informatici*, in Cass. pen., 2001, (7), p. 2244 ss; Pecorella, *L'attesa pronuncia delle sezioni unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*, in Cass. pen., 2012, (11), p. 3681 ss.; Perri, *Un'introduzione alle investigazioni scientifiche,* in Ciberspazio e diritto, 2008, (2), p. 145 ss.; Picotti, *Reati informatici (voce),* in Enc. giur. Treccani, agg. VIII, Roma, 2000, p. 1; . Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), Il diritto penale dell'informatica nell'epoca di internet, Trento, 2004, p. 21 ss.; Salvadori, *Hacking, cracking e nuove forme di attacco ai sistemi d'informazione. Profili di diritto penale e prospettive de jure condendo*, in Ciberspazio e diritto, 2008, (3), p. 329 ss.; Santoriello - Dezzani, *Il reato di accesso e trattenimento "abusivi" nel sistema informatico e la responsabilità amministrativa delle persone giuridiche*, in La

2.2.a) premessa.

Alla diffusione commerciale dei cc.dd. "personal computers" (o sistemi informatici per uso privato), a partire dalla fine degli anni '80 in poi, si è accompagnato un sempre più accentuato sviluppo delle reti informatiche e telematiche, che sta conoscendo il proprio apice con la propagazione a livello mondiale della rete Internet la quale ha prodotto e (sta tuttora producendo) enormi cambiamenti nelle dinamiche dei rapporti umani non soltanto a livello tecnologico, ma soprattutto a livello culturale, sociale ed anche giuridico.
Contestualmente all'evoluzione di tale tecnologie si è avuta la nascita e la proliferazione di molte nuove forme di reato e di aggressioni criminose, talvolta commesse per mezzo di sistemi informatici e telematici, talaltra contro i sistemi stessi, intesi non più come strumenti per compiere tali reati, sibbene proprio come oggetto materiale di quest' ultimi. Ed è in questa seconda accezione che si suole parlare di cc.dd. "*computer crimes*" (o *cybercrimes*).
Alcuni autori sono soliti distinguere tra reati commessi su Internet e reati commessi mediante Internet. Al primo gruppo apparterebbero la maggior parte dei reati introdotti con la legge 23 dicembre 1993 n. 547 (cc.dd reati informatici o telematici propri)[99]. Il secondo gruppo coincide invece con un complesso eterogeneo e difficilmente classificabile di reati comuni, previsti dal codice penale, da leggi speciali ovvero contemplati dalla stessa legge n°547 (cc.dd. reati informatici o telematici impropri).
Definita questa prima ampia, duplice categoria di reati, ci si limiterà nel prosieguo ad una breve e sintetica disamina delle principali fattispecie criminose riconducibili alla predetta bipartizione, anticipando sin da adesso l'assenza di qualsivoglia pretesa di completezza od originalità, alla stregua della considerazione che trattandosi essenzialmente di problematiche afferenti esclusivamente al diritto penale sostanziale, la conoscenza delle stesse (d'altra parte irrinunciabile) può cionondimeno aiutare a meglio definire e delimitare, nell'ambito di questo lavoro, l'alveo delle circostanze e delle situazioni al verificarsi delle quali il ricorso (anche) ad intercettazioni telematiche può presentarsi, dal punto di vista investigativo, come presupposto indefettibile al fine di accertare l'esistenza stessa di reati ed eventualmente ad individuarne gli autori.

2.2.b) La genesi dei reati informatici nell'ordinamento italiano.

Prima della legge n. 547 del 1993, nel nostro ordinamento non esisteva alcuna disposizione normativa specifica sui reati informatici (o *computer crimes*). A

---

responsabilità amministrativa delle società e degli enti, 2012, (1), p. 57 ss.; Sarzana Di S. Ippolito, *Informatica, internet e diritto penale,* Milano, 2010; Scognamiglio, *Criminalità informatica,* Napoli, 2008; Scuderi, *Un caso di hacking: luoghi reali e luoghi virtuali tra diritto e informatica*, in Ciberspazio e diritto, 2006, (7), p. 377 ss.; Strano, *Computer crime*, Milano, 2000;

[99] Vedi *supra* para. 1.3.a);

fronte della necessità di approntare un'adeguata tutela giuridica in presenza di nuove forme di aggressione "tecnologica", si era posto il problema dell'applicabilità in via estensiva e, soprattutto, analogica delle norme penali preesistenti. I principi di legalità e tassatività, peraltro, correlati con il divieto dell'analogia in *malam partem* nel diritto penale ex art. 14 disp. prel. c.c. (ed anche artt. 1 e 199 c.p.) rendevano questa strada difficilmente percorribile.

Parimenti, in quel periodo, era sorta altresì l'esigenza di uniformare e parificare il diritto positivo italiano a quello di altri ordinamenti stranieri, anche per consentire, ai fini della cooperazione ed estradizione internazionale, la c.d. doppia incriminazione (stesso fatto punito in due o più ordinamenti). A tal uopo, le fattispecie relative ai *computer crimes* venivano quindi ricondotte, con evidenti difficoltà e forzature tecnico giuridiche, nell'ambito applicativo delle preesistenti norme incriminatrici (come quelle sul furto, sul danneggiamento, sulla frode o sulla truffa). In tale contesto, le uniche due disposizioni che venivano ritenute pacificamente suscettibili di applicazione ai *computer crimes* erano l'art. 12 L. 121/1981[100] ("Nuovo ordinamento dell'Amministrazione della Pubblica Sicurezza") e l'art. 420 c.p., rubricato "Attentato ad impianti di pubblica utilità", così come modificato dalla L. 191/1978.

Nel 1993, di conseguenza (come più volte ricordato *supra*), il legislatore italiano ha ritenuto di dover intervenire a colmare la predetta lacuna con la già citata L. 23 dicembre 1993 n. 547, mediante la quale, da un lato, ha introdotto nuove forme di aggressione criminosa - inserendole per coerenza sistematica all'interno del codice penale (e operando quindi la scelta di non considerare i reati informatici come aggressivi di beni giuridici nuovi rispetto a quelli tutelati dalle norme incriminatrici preesistenti) e, dall'altro, ha previsto nuovi e più idonei strumenti investigativi (attraverso appunto l'inserimento di un nuovo art. 266 bis nel c.p.p.).

Volendo soddisfare confacenti intenti schematici, potremmo asserire che la legge 547/93 è intervenuta in quattro diverse direzioni, punendo le seguenti forme di aggressione:

- le aggressioni alla **riservatezza** dei dati e delle comunicazioni informatiche;
- le aggressioni **all'integrità** dei dati e dei sistemi informatici;
- le condotte in tema di **falso**, estese ai documenti informatici;
- le **frodi** informatiche.

2.2.c) L' accesso abusivo ad un sistema informatico o telematico.

Una delle più importanti novità introdotte dalla l. 547/93 è senz'altro l'art. 615 *ter* c.p. che è principalmente finalizzata a contrastare il dilagante fenomeno degli

[100] Art.12 l.n°121/1981: *"Il pubblico ufficiale che comunica o fa uso di dati o informazioni in violazione delle disposizioni della presente legge, o al di fuori dei fini previsti dalla stessa, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a tre anni. Comma 2…(omissis)."*

"hacker"[101]. Si tratta di un reato comune, perpetrabile da chiunque: è sufficiente che il soggetto attivo abbia delle conoscenze tecniche (anche minime!) affinché le condotte possano essere integrate. La norma prevede, in via alternativa, due condotte: a) l'introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza; b) il mantenersi nel medesimo sistema contro la volontà espressa o tacita di chi ha il diritto di escluderlo. Nella prima ipotesi il legislatore ha voluto punire un'azione immateriale consistente nell'introdursi ed accedere alla memoria di un elaboratore per prendere cognizione di dati, informazioni e programmi, ovvero per alterarli, modificarli o cancellarli. Tale accesso deve verificarsi in presenza di misure di sicurezza minime, cioè misure tecniche, informatiche, organizzative e procedurali volte ad escludere o impedire la cognizione delle informazioni a soggetti non autorizzati. Tra queste rientrano le password (di almeno 8 caratteri secondo il T.U. della Privacy), dispositivi biometrici, firewall, etc. Chiaramente le misure devono riferirsi all'elaboratore e non ai locali dove esso è ospitato. L'accesso deve essere abusivo, compiuto cioè da chi non è autorizzato ad introdursi nel sistema. La seconda ipotesi si riferisce invece al mantenimento nel sistema informatico nonostante il titolare abbia espresso, in maniera espressa o tacita, la volontà di esclusione (*cd. ius excludendi*). L'oggetto materiale del reato può essere il sistema informatico ovvero quello telematico. Nonostante la mancanza di una specifica definizione, nel primo termine rientra pacificamente l'hardware (elementi fisici costituenti l'unità di elaborazione), il software (programmi di funzionamento) e tutti gli apparati che permettono di inserire (scanner, lettore DVD, etc.) o estrapolare (stampante, casse, masterizzatore, etc.) dati e informazioni. Il sistema telematico può essere invece definito come una serie di componenti informatici collegati tra di loro mediante tecnologie di comunicazione. L'oggetto giuridico tutelato dalla norma è, secondo la teoria predominante, il "domicilio informatico". Ancora, l'art. 615 ter è collocato tra i delitti contro la inviolabilità del domicilio, perché si è ritenuto che i sistemi informatici costituiscano *"un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli artt. 614 e 615 del codice penale"*[102]. Secondo alcuni, quindi, il legislatore avrebbe riconosciuto, accanto alla nozione classica di domicilio rilevante per il diritto penale, una nuova figura chiamata "domicilio informatico", in considerazione del fatto che i sistemi informatici e telematici costituiscono innanzitutto dei luoghi ove l'uomo esplica alcune delle sue facoltà intellettuali ed esprime la propria personalità, con facoltà di escludere terzi non graditi. L'elemento psicologico richiesto è il dolo generico. La Cassazione ha avuto modo di precisare che *"l'accesso abusivo a un sistema telematico o informatico si configura con la mera intrusione e non richiede che la condotta comporti una lesione della riservatezza degli utenti né tantomeno che "l'invasione" sia compiuta con l'obiettivo di violare la loro privacy"*[103].

---

[101] Vedi *supra* n.44 para. 1.3.a)

[102] Così la Relazione sul disegno di legge n. 2773, poi tradottosi nella l. 547/93.

[103] Cass. Sent. 6 febbraio 2007, n. 11689.

Spingendosi più in là, i giudici di legittimità hanno da ultimo ricostruito la configurabilità del reato di intrusione abusiva in un sistema informatico o telematico anche nell'ipotesi in cui il soggetto, abilitato per motivi di servizio o di ufficio ad accedere ad una banca dati e in possesso delle necessarie credenziali di autenticazione (es. user-id e password) del predetto sistema informatico o telematico, decida di entrare nel sistema non per motivi di ufficio bensì per motivi diversi - non autorizzati dal complesso delle prescrizioni che regolano e disciplinano l'accesso - del tutto personali o per altre finalità (cessione a terzi dei dati o delle informazioni, curiosità personale, vendita di dati, corruzione di pubblici ufficiali, rivelazione di segreti di ufficio o aziendali)[104].

2.2.d) Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater* c.p.) e diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 *quinquies* c.p.).

La prima norma, com'è evidente, configura un mero reato di pericolo ed è preordinata ad anticipare la tutela rispetto al verificarsi di un evento dannoso. L'art. 615 quater vuole infatti punire chiunque riesca ad impossessarsi o diffonda codici di accesso riservato necessari ad entrare in un sistema informatico o telematico. Anomalia di tale norma è il fatto che la rubrica dell'art. 615 *quater* parla espressamente di detenzione, mentre il testo della norma dimentica del tutto tale condotta.

In questa figura di reato rientrano ad esempio i casi di clonazione di cellulari (consistenti nella duplicazione abusiva del numero seriale del cellulare)[105].

Detta norma non ha mancato di sollevare qualche perplessità interpretativa in relazione a quei siti, italiani (come spysystem.it) e stranieri (come astalavista.com), che mettono a disposizione degli utenti una serie di strumenti, sotto forma di programmi e manuali, idonei a realizzare un accesso abusivo ad un sistema informatico. Si riconosce infatti che il servizio così offerto non integra gli estremi della

[104] SS.UU. Sent. n°4694 del 7 febbraio 2012. Nel caso specifico, i Giudici Ermellini hanno confermato la condanna emessa dalla Corte d'Appello di Roma nei confronti di un maresciallo dei carabiniere che, nonostante avesse accesso ad un database investigativo riservato agli appartenenti dell'Arma (*S.D.I. "Sistema di Indagine"*) tramite regolare password, si era tuttavia servito del sistema, in un momento in cui non risultava in servizio, non al fine della conduzione di un'indagine ufficiale, bensì per meri scopi privati, in particolare per svelare informazioni riservate ad una sua conoscente per aiutarla in vista di un procedimento di separazione.

[105] La Cassazione con Sent. del 17 dicembre 2004, n. 5688, ha infatti avuto modo di precisare che *"integra il reato di detenzione e diffusione abusiva di codici di accesso a servizi informatici o telematici di cui all'art. 615 quater c.p., la condotta di colui che si procuri abusivamente il numero seriale di un apparecchio telefonico cellulare appartenente ad altro soggetto, poiché attraverso la corrispondente modifica del codice di un ulteriore apparecchio (cosiddetta clonazione) è possibile realizzare una illecita connessione alla rete di telefonia mobile, che costituisce un* ***sistema telematico protetto****, anche con riferimento alle banche concernenti i dati esteriori delle comunicazioni, gestite mediante tecnologie informatiche"*

fattispecie di cui all'art. 615 quater, richiedendo la disposizione in esame il *dolo specifico* del *"procurare a sé o ad altri un ingiusto profitto o di arrecare ad altri un danno"*, mentre in tal caso il fine perseguito (e di solito dichiarato dallo stesso curatore del sito) è esclusivamente didattico-informativo: rendere comprensibile un fenomeno a chi intende studiarlo. Eppure, si osserva, dal momento che la norma è funzionalmente collegata alla disposizione di cui all'art. 615 ter *(supra)*, reato per realizzare il quale è imprescindibile una previa acquisizione di strumenti idonei di accesso, non si capisce come possa assumere un'autonoma rilevanza.

L'art. 615 *quinquies* c.p. riguarda invece la fattispecie della diffusione di programmi idonei a danneggiare un sistema informatico. La norma punisce infatti chiunque *diffonda, comunichi o consegni* un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.
Tale norma, benché impropriamente collocata tra i delitti contro l'inviolabilità del domicilio, mira in realtà a tutelare l'integrità e la funzionalità dei sistemi informatici. L'oggetto materiale sul quale si focalizzano le diverse modalità di porsi delle condotte precedentemente menzionate (e contenute nella norma in esame) si sostanzia, in definitiva, in un programma per elaboratore per così dire *"infetto"*. Con tale espressione si intende fare riferimento non solo al programma in grado di *danneggiare* le componenti logiche di un sistema informatico, ma anche a quello diretto ad interromperne o alterarne il funzionamento.

2.2.e) segue: i cc.dd. programmi *"nocivi"* (*malware, virus*, *worm*, *trojan*, *backdoor*, *spyware*, *dialer*, *etc*.).

Esiste una vasta congerie ed un'ampia varietà di programmi cc.dd. *"nocivi"*. Ora, considerato che la comunità degli *hackers* (*rectius, cracker*s) è alla continua ricerca di modalità tecniche innovative preordinate al raggiungimento dei fini (sovente criminali) che gli stessi appartenenti al gruppo si propongono di perseguire, una qualsiasi elencazione di detti congegni operativi sarebbe per ciò solo incompleta e di fatto superata dallo stato attuale della tecnica. Cionondimeno, la consultazione di siti web tra i più attenti ed aggiornati sulla problematica in argomento - quali ad esempio le pagine della più vasta enciclopedia *online* esistente (Wikipedia) - permette comunque di ottenere una panoramica soddisfacente dei *tools* e delle metodologie adottate al fine di violare sistemi informatici altrui per gli scopi (legali e non) più diversi. Per di più, ai fini del presente lavoro, l'importanza della conoscenza dei diversi tipi di detti programmi informatici, si rileva dalla circostanza che gli stessi espedienti tecnici sono sovente alla base delle stesse azioni investigative degli organi

inquirenti, quando ad esempio si tratta di porre in essere un'intercettazione telematica od informatica[106].

Malware, ad esempio, è espressione generica per indicare un qualsiasi *software* creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* e ha dunque il significato letterale di *"programma malvagio";* in italiano è detto anche codice maligno.

Il *virus* è un software appartenente alla categoria dei *malware* che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente. Un virus è composto da un insieme di istruzioni, come qualsiasi altro programma per computer. È solitamente composto da un numero molto ridotto di istruzioni (da pochi byte ad alcuni kilobyte), ed è specializzato per eseguire soltanto poche e semplici operazioni e ottimizzato per impiegare il minor numero di risorse, in modo da rendersi il più possibile invisibile. Caratteristica principale di un *virus* è quella di riprodursi e quindi diffondersi nel computer ogni volta che viene aperto il *file* infetto.

Un ***worm*** (letteralmente "verme") è una particolare categoria di *malware* in grado di autoreplicarsi. È simile ad un *virus*, ma a differenza di questo non necessita di legarsi ad *altri* file eseguibili per diffondersi. Tipicamente un *worm* modifica il computer che infetta, in modo da venire eseguito ogni volta che si avvia la macchina e rimanere attivo finché non si spegne il computer o non si arresta il processo corrispondente. Il mezzo più comune impiegato dai *worm* per diffondersi è la posta elettronica: il programma maligno ricerca indirizzi e-mail memorizzati nel computer ospite ed invia una copia di sé stesso come *file* allegato (*attachment*) a tutti o parte degli indirizzi che è riuscito a raccogliere. I messaggi contenenti il *worm* utilizzano spesso tecniche di *social engineering*[107] per indurre il destinatario ad aprire l'allegato, che spesso ha un nome che permette al *worm* di camuffarsi come *file* non eseguibile. Alcuni *worm* sfruttano dei *bug*[108] di *client* di posta molto diffusi, come Microsoft Outlook Express, per eseguirsi automaticamente al momento della visualizzazione del messaggio e-mail. Questi eseguibili maligni possono anche sfruttare i circuiti del *file sharing* per diffondersi. In questo caso si copiano tra i *file* condivisi dall'utente vittima, spacciandosi per programmi ambìti o per *crack* di programmi molto costosi o ricercati, in modo da indurre altri utenti a scaricarlo ed eseguirlo.

Un ***trojan*** o ***trojan horse*** (Cavallo di Troia in inglese), è un tipo di *malware*. Esso deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice *trojan* nascosto. L'attribuzione del termine "Cavallo di Troia" ad un programma o,

---

[106] In tal senso cfr. il para. 3.1.e) in tema di intercettazione delle conversazioni voip, *infra*.

[107] Nel campo della sicurezza delle informazioni per "ingegneria sociale" (dall'inglese *social engineering*) si intende lo studio del comportamento individuale di una persona al fine di carpirne informazioni utili. Per un'ampia analisi del fenomeno cfr. nota 231, *infra.*

[108] Per la nozione di *bug* cfr. nota n°17.

comunque, ad un *file* eseguibile, è dovuta al fatto che esso nasconde il suo vero fine. È proprio il celare le sue reali "intenzioni" che lo rende un *trojan*. I *trojan* non si diffondono autonomamente come i *virus* o i *worm*, quindi richiedono un intervento diretto dell'aggressore per far giungere l'eseguibile maligno alla vittima.

Le ***backdoors*** in informatica sono paragonabili a porte di servizio che consentono di superare, in parte o in tutto, le procedure di sicurezza attivate in un sistema informatico. Queste "porte" possono essere intenzionalmente create dai gestori del sistema informatico per permettere una più agevole opera di manutenzione dell'infrastruttura informatica, e più spesso da *crackers* intenzionati a manomettere il sistema. Possono anche essere installate autonomamente da alcuni *malware* (come *virus*, *worm* o *trojan*), in modo da consentire ad un utente esterno di prendere il controllo remoto della macchina senza l'autorizzazione del proprietario.

Uno ***spyware*** è un tipo di *software* che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete, etc.) senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, solitamente attraverso l'invio di pubblicità mirata. In un senso più ampio, il termine *spyware* è spesso usato per definire un'ampia gamma di *malware* dalle funzioni più diverse, quali l'invio di pubblicità non richiesta (*spam*), la modifica della pagina iniziale o della lista dei Preferiti del browser, oppure attività illegali quali la re-direzione su falsi siti di e-commerce (c.d *phishing*) o l'installazione di *dialer* truffaldini per numeri a tariffazione speciale. Gli *spyware*, a differenza dei *virus* e dei *worm*, non hanno la capacità di diffondersi autonomamente, quindi richiedono l'intervento dell'utente per essere installati. In questo senso sono dunque simili ai *trojan*.

I ***dialer***, letteralmente “compositori di numeri telefonici”, rappresentano in ambito commerciale un tramite per accedere a servizi a sovrapprezzo o a tariffazione speciale. In particolare, il “*dialer*” è uno speciale programma autoeseguibile che altera i parametri della connessione a Internet impostati sul computer dell'utente, agendo sul numero telefonico del collegamento e sostituendolo con un numero a pagamento maggiorato su prefissi internazionali satellitari o speciali. Una percentuale della somma fatturata per la chiamata/connessione viene girata dal gestore telefonico ad una terza società titolare delle numerazioni indicate.

Il termine ***hijacker*** o *browser hijacker* ("dirottare” in inglese) o *highjacker* indica un tipo di *malware* che prende il controllo di un *browser* al fine di modificarne la pagina iniziale o farlo accedere automaticamente a siti indesiderati. Nei sistemi Windows, un *hijacker* agisce spesso sui registri di sistema (cosa che può rendere molto difficile la sua identificazione da parte di utenti inesperti). Può coesistere o cooperare con altri tipi di *malware*: per esempio, una manomissione del sistema a scopo di *hijacking* può essere eseguita da un *trojan horse*; oppure, un *hijacker* può dirottare il *browser* su pagine con contenuti dinamici che consentono altri tipi di attacco al computer (*dialer*, *virus*, o per scopi di *spam* pubblicitario e così via).

Un ***rootkit*** è un programma software creato per avere il controllo completo sul sistema senza bisogno di autorizzazione da parte di utente o amministratore. Recentemente alcuni *virus* informatici si sono avvantaggiati della possibilità di agire

come *rootkit* (processo, *file*, chiave di registro, porta di rete) all'interno del sistema operativo.
Un ***keylogger***, infine, è, nel campo dell'informatica, uno strumento in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio computer. Spesso i *keylogger software* sono trasportati ed installati nel computer da *worm* o *trojan* ricevuti tramite Internet ed hanno in genere lo scopo di intercettare *password* e numeri di carte di credito ed inviarle tramite posta elettronica al creatore degli stessi. Un programma di *keylogging* può sovrapporsi fra il *browser* ed il *World Wide Web*. In questo caso intercetta le *password*, comunque esse vengano inserite nel proprio PC. La password viene catturata indipendentemente dalla periferica di *input* (tastiera, mouse, microfono): sia che l'utente la digiti da tastiera, sia che l'abbia salvata in un file di testo prima di collegarsi a Internet, e poi si limiti a fare copia/incolla, in modo da evitarne la digitazione, sia questa venga inserita da un programma di dettatura vocale. Anche in caso di connessione sicura (cifrata), se sul computer è presente un *keylogger* che invia le *password* in remoto, tali *password* potranno essere utilizzate dalla persona che le riceve.

2.2.f) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche telematiche (art. 617*quater).*

In base all'art. 617 *quater* c.p. è punito con la reclusione da sei mesi a quattro anni *"chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe"*; la stessa pena è poi prevista, dal secondo comma, per *"chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma".*
Per "intercettazione" deve intendersi la presa di cognizione, totale o parziale, della comunicazione, purché, in questo secondo caso, la parte appresa abbia una giuridica rilevanza, ancorché minima. La comunicazione, comunque, deve pervenire integralmente al legittimo destinatario, perché, diversamente, ricorrerebbero le altre ipotesi previste dalla norma quali quella di "interruzione" - che appunto si realizza qualora la comunicazione sia iniziata e, successivamente, fatta cessare - oppure, quella di "impedimento" che, invece, esclude anche il mero inizio della comunicazione.
La norma richiede che la condotta sia realizzata *"fraudolentemente".* All'uopo sono emerse due distinte tesi: la prima, riferisce l'avverbio alla sola intercettazione, la seconda, lo estende all'impedimento e all'interruzione[109].
La condotta può definirsi "fraudolenta" quando consiste in un'attività volta a rappresentare, al sistema stesso in via automatica o al gestore del sistema, una

[109] Nel senso che l'avverbio "fraudolentemente" sia riferito anche alle altre due modalità della condotta, Fondaroli D., *La tutela penale dei beni informatici, in Diritto dell'informazione e dell'informatica,* 1996, pag. 316;

situazione non corrispondente al vero quanto, ad esempio, all'identità del soggetto autorizzato o alle caratteristiche del sistema intercomunicante o dell'impianto ricevente o comunque tale da rendere non percettibile o riconoscibile l'intromissione abusiva. La fraudolenza deve intendersi quale modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione. Di converso, la fattispecie non trova applicazione se il soggetto, il cui messaggio è intercettato, è consapevole dell'intromissione del terzo. Deve però trattarsi di una consapevolezza non appresa casualmente o indirettamente. In altri termini, solo se l'agente ha reso manifesta la volontà di intercettare la comunicazione ed ha in tal modo consentito all'interessato di averne conoscenza prima che l'azione sia posta in essere, il reato è escluso.

Si tratta, inoltre, almeno per le condotte di cui al primo comma, di un reato unico, anche nel caso in cui l'agente realizzi contestualmente più di un'ipotesi criminosa. La norma, peraltro, così come congegnata dal legislatore, non è esente da talune aporie. Ciò è ad esempio messo in evidenza al ricorrere di ipotesi – oggi sempre più frequenti - di *net-strike*[110]: anche ritenendo che l'art. 617 quater sia volto a garantire la sicurezza delle comunicazioni informatiche e telematiche, pare assurdo pensare di punire decine, centinaia o migliaia di utenti che per qualsiasi ragione si collegano contemporaneamente ad un dato sito eventualmente saturandone le risorse. Il "corteo telematico", infatti, costituisce il più delle volte una manifestazione pacifica, pubblica e tendenzialmente legittima: non presenta in se carattere distruttivo e le sue più estreme conseguenze consistono in un blocco temporaneo del *server* che può essere rimesso in piena attività al termine della protesta stessa. Se la norma dovesse essere applicata alla lettera, occorrerebbe promuovere un procedimento nei confronti di tutti quelli che vi partecipano, assurdità palese se solo si considera che è impossibile distinguere tra utenti che si collegano al sito bersaglio aderendo alle motivazioni della manifestazione ed utenti la cui richiesta ai servizi del sito è, rispetto alle predette motivazioni, del tutto estranea.

L'ipotesi di cui al secondo comma, relativa alla "rivelazione" mediante mezzi di informazione al pubblico, rappresenta invece una fattispecie sussidiaria, autonoma rispetto ai fatti descritti al primo comma.

La Cassazione ha statuito che integra la violazione di cui all'art. 617quater, comma 2 c.p., la condotta di chi diffonda al pubblico una trasmissione televisiva interna, trasmessa da punto a punto (c.d. "fuori onda") su un canale riservato a comunicazioni di servizio, ed intercettata in modo fraudolento. Il caso si riferiva a Striscia la notizia che aveva “intercettato” dei fuori onda poi trasmessi nel corso della propria trasmissione[111].

[110] Letteralmente:inscenamento di atti di protesta sulla rete.

[111] Cass. Pen. 19 maggio 2005, n. 4011.

2.2.g) L'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.) e la falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617 *sexies* c.p.).

Le stesse comunicazioni informatiche sono tutelate, nei confronti di una condotta prodromica rispetto a quella prevista dalla norma precedente, attraverso l'art. 617 quinquies c.p., che commina la pena della reclusione da uno a quattro anni per *"chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi".*

A differenza di quanto previsto dall'art. 617 bis c.p. per le comunicazioni telegrafiche e telefoniche, l'intercettazione, l'impedimento o l'interruzione delle comunicazioni in corso non costituiscono più soltanto l'oggetto del dolo specifico - in quanto particolare finalità alla quale deve essere rivolta la condotta dell'agente – ma, inequivocabilmente, rilevano già sul piano del fatto, richiedendo espressamente la norma che gli apparecchi siano atti ad intercettare comunicazioni. L'art. 617 quinquies c.p. configura, quindi, un reato di pericolo concreto, dovendo il giudice accertare, di volta in volta, che l'apparecchiatura installata sia idonea a realizzare l'evento lesivo. In altri termini, la condotta vietata è rappresentata dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate: la condotta non realizza alcuna concreta lesione del bene protetto, ma si limita a rendere probabile il verificarsi di quest'ultima. Si tratta, quindi, di un reato di pericolo per la cui configurazione non è necessaria la prova dell'avvenuta intercettazione o interruzione o impedimento della comunicazione, essendo sufficiente accertare l'obbiettiva potenzialità lesiva dell'apparecchiatura. Pertanto, nel caso in cui chi predispone dette apparecchiature proceda ulteriormente all'intercettazione, interruzione, impedimento o rivelazione delle comunicazioni, troveranno applicazione più fattispecie criminose[112].

Va all'uopo segnalata una pronuncia del GIP presso il Tribunale di Milano[113] secondo cui integra il reato di cui all'art. 617 quinquies c.p. e non il reato di cui all'art. 617 quater c.p. la condotta di chi installa su uno sportello bancomat, in sostituzione del pannello originario, una apparecchiatura composta da una superficie plastificata, con una microtelecamera con funzioni di registratore video per la rilevazione dei codici bancomat, quando non vi sia prova certa dell'avvenuta captazione di almeno un codice identificativo. L'attività illecita di intercettazione, infatti, nel silenzio dell'art. 617 quinquies c.p., deve ritenersi possa essere consumata con qualunque mezzo ritenuto idoneo a svelare la conoscenza di un sistema informatico qual è da considerarsi la digitazione da parte dell'operatore umano del codice di accesso ad un

[112] L'art. 617 *quinquies* c.p. può quindi concorrere materialmente con le due fattispecie di reato di cui al primo e secondo comma dell'art. 617 *quater*.

[113] Sent. del 19 febbraio 2007.

sistema attraverso una tastiera alfanumerica, digitazione che era destinata ad essere l'oggetto dell'illecita captazione.

La seconda norma (art. 617 *sexies* c.p.) punisce invece il comportamento di chi falsifica, altera o sopprime il contenuto delle comunicazioni informatiche o telematiche. Per configurare il reato è necessario soltanto che l'agente, oltre a porre in essere le condotte appena descritte, faccia o permetta che altri ne facciano un uso illegittimo di tali comunicazioni. E' richiesto inoltre, come evidente, il dolo specifico.

2.2.h) L'integrità dei sistemi informatici e telematici.

Dopo aver brevemente esaminato le norme incriminatrici in tema di *accesso* al sistema informatico e telematico, bisogna ora volgere l'attenzione alla tutela apprestata dalla legge penale in materia di *integrità* dei sistemi informatici e telematici. Il primo reato che va a tal uopo esaminato è quello previsto dall'art. 635 *bis* c.p. e rubricato *"Danneggiamento di sistemi informatici o telematici"*. L'art. 635 bis non si limita ad ampliare ed integrare la norma sul danneggiamento (art. 635 c.p.), con riguardo ai dati ed ai programmi, ossia alle componenti immateriali di un sistema informatico, ma predispone altresì una tutela rafforzata di tutti i beni informatici, prevedendo un trattamento più rigoroso, sia sotto il profilo sanzionatorio che sotto il profilo della procedibilità, anche di fatti che erano pacificamente riconducibili alla fattispecie tradizionale, in quanto aventi ad oggetto cose materiali: il sistema informatico o telematico, ovvero il supporto materiale delle informazioni.
Oggetto di danneggiamento può essere innanzitutto il sistema informatico, eventualmente collegato a distanza con altri elaboratori, come nel caso dei sistemi telematici e l'aggressione può riguardare tanto il sistema nel suo complesso quanto una o più delle sue componenti materiali, quali il video, la tastiera, etc.
Il danneggiamento, inoltre, può riguardare anche i dati e i programmi informatici nonché le informazioni contenute nel sistema. L'art. 635 *bis* richiede che i beni informatici oggetto di aggressione siano "altrui": il problema del significato da attribuire a tale termine sembra destinato ad assumere rilevanza pratica proprio in relazione alla nuova figura di danneggiamento informatico, stante la diffusa prassi di procurarsi la disponibilità di hardware e di software attraverso contratti di locazione (anziché di compravendita), solitamente accompagnati dalla contestuale conclusione di un contratto di assistenza e/o manutenzione con lo stesso fornitore. Il danneggiamento si può attuare nella distruzione, nel deterioramento e nella inservibilità totale o parziale. Nessun problema nel caso di distruzione intesa nel senso di eliminazione materiale del sistema informatico o telematico ovvero delle informazioni contenute su un supporto materiale. Diverso è il caso della distruzione di dati e programmi che, oltre all'annientamento del supporto fisico, può anche risultare dalla cancellazione. Tale ultima ipotesi può essere attuata: a) attraverso la smagnetizzazione del supporto; b) attraverso la sostituzione dei dati originari con dati

nuovi; c) impartendo all'elaboratore il comando di provocare la scomparsa dei dati. In questi casi, comportando la distruzione una eliminazione totale del bene aggredito, non troverà applicazione la norma incriminatrice allorquando i dati o i programmi siano ancora recuperabili ovvero ne sia stata soltanto impedita la visualizzazione. Il deterioramento comporterà invece solo una apprezzabile diminuzione del valore o della utilizzabilità dei dati e dei programmi. L'inservibilità totale o parziale del sistema informatico o telematico riguarda tutte quelle situazioni di compromissione totale o parziale del funzionamento del sistema, che possono avere ad oggetto sia le parti meccaniche che quelle logiche (ad es. nel caso di introduzione di un programma *worm*).

2.2.i) segue: il concetto di violenza su sistema informatico e/o telematico.

Il terzo comma, introdotto dalla L. 547/93, prevede che la "violenza sulle cose" possa configurarsi anche nel caso in cui *un programma informatico venga alterato, modificato, cancellato in tutto o in parte ovvero venga impedito o turbato il funzionamento di un sistema informatico o telematico*.
Con l'aggiunta del terzo comma, il legislatore ha voluto tutelare nuove e specifiche modalità di aggressione, che riflettono le forme tipiche di aggressione ai programmi informatici. Un programma informatico potrà dirsi *alterato* quando ne è stata modificata l'essenza attraverso una manipolazione totale o parziale delle istruzioni che lo componevano. Si avrà una *modificazione* del programma ogniqualvolta l'intervento abusivo compiuto su di esso si esaurisca nel renderlo in tutto o in parte diverso, senza peraltro snaturarne le originarie funzioni. La *cancellazione* di un programma consiste infine nella soppressione totale o parziale delle istruzioni che lo compongono.
La seconda nuova ipotesi di violenza sulle cose ha ad oggetto il funzionamento di un sistema informatico o telematico; ricadranno in questa previsione tutte quelle forme di "disturbo" del processo di elaborazione o di trasmissione a distanza di dati, che non consistano in un intervento diretto sul programma.
Si avrà impedimento del funzionamento del sistema qualora, per es., siano stati disattivati i collegamenti elettrici e/o elettronici del computer, rendendo oltremodo difficile all'utente ripristinarli o quanto meno individuare la causa della paralisi. L'ipotesi del turbamento del funzionamento del sistema sarà integrata da un'azione di disturbo del regolare svolgimento delle operazioni dell'elaboratore, tale da causare un pregiudizio al legittimo utente del sistema[114].

[114] La Pretura di Torino nel'ambito di una risalente sentenza del 15 maggio 1996 stabilì che *"deve ritenersi violenza sulle cose, tale da integrare l'elemento della fattispecie di cui all'art. 392 comma ultimo c.p.*(esercizio arbitrario delle proprie ragioni con violenza sulle cose n.d.r)*, il comportamento di un soggetto il quale, al fine di esercitare un preteso diritto di esclusiva per l'installazione e gestione delle componenti informatiche di macchinari industriali, altera surrettiziamente il programma di propria produzione installato sugli stessi, inserendo un file di "blocco data" in grado di interrompere*

2.2.l) Attentato a impianti di pubblica utilità (art. 420 c.p.).

L'elemento oggettivo è costituito dalla distruzione o dal danneggiamento di impianti di pubblica utilità o di ricerca ed elaborazione dei dati, ovvero di sistemi informatici o telematici di pubblica utilità, ovvero ancora di dati, informazioni o programmi in essi contenuti o ad essi pertinenti. L'inserimento della "pubblica utilità" quale ulteriore elemento costitutivo della fattispecie criminosa serve a restringere il campo di applicazione della norma, facendo sì che gli impianti interessati siano solo quelli la cui messa fuori uso possa determinare un pericolo per l'ordine pubblico. La pubblica utilità, infatti, è generalmente intesa in senso funzionale, risolvendosi cioè nella destinazione al servizio di una collettività indifferenziata di persone, con il correttivo del criterio dimensionale che postula l'indeterminatezza della quantità di soggetti che fruiscono dei dati del sistema.

2.2.m) La rilevanza penale del documento informatico.

Con l'introduzione dell'*art. 491bis c.p.* ed il *secondo comma dell'art. 621 c.p.* esordisce, nel campo penale, la figura del *documento informatico*, peraltro in anticipo rispetto alla più organica disciplina amministrativa e civile.
Di fronte al sempre maggior utilizzo di sistemi informatici, in grado anche di rappresentare manifestazioni di volontà o di scienza del compilatore (si pensi ad un comunissimo documento di testo contenente delle dichiarazioni e redatto utilizzando Word), il legislatore è dovuto intervenire per salvaguardare l'affidabilità e la certezza dei dati informatici nei rapporti giuridici. Il falso informatico è stato quindi assimilato in tutto e per tutto al falso documentale, inserendo uno specifico articolo nel codice penale (491bis) che ha esteso, mediante un indiscriminato rinvio, tutte le fattispecie incriminatrici in tema di falso al *"documento informatico"* (vd., come detto, anche art. 621, 2° c., c.p.). L'introduzione dell'art. 491 bis risponde quindi alla necessità di assicurare una sanzione penale alle diverse forme di falso informatico che non erano riconducibili alle norme sui falsi documentali. Alla nozione "tradizionale" di documento, infatti, il documento informatico risultava essenzialmente estraneo, soprattutto per il fatto di non essere redatto in quella forma scritta alfabetica che caratterizza i documenti tradizionali.
Questa tecnica legislativa si è basata sulla considerazione che nel falso informatico cambia solo l'oggetto materiale del reato, costituito non più da un supporto cartaceo o comunque fisico bensì informatico. Tale scelta si è però rivelata non del tutto indovinata, tanto da essere successivamente (come vedremo *infra*) abbandonata.

---

automaticamente il funzionamento del macchinario - rendendolo del tutto inservibile - alla scadenza della data prestabilita".

2.2.n) La frode informatica (art. 640 *ter* c.p.).

L'art. 640 *ter* c.p. è diretto a reprimere le ipotesi di illecito arricchimento conseguito attraverso l'impiego fraudolento di un sistema informatico. L'interferenza può realizzarsi in una qualsiasi delle diverse fasi del processo di elaborazione dei dati: dalla fase iniziale - di raccolta e inserimento dei dati da elaborare *(cd. manipolazione di input)* - alla fase intermedia, volta alla elaborazione in senso stretto *(cd. manipolazione di programma),* alla fase finale, di emissione, in qualsiasi forma, dei dati elaborati *(cd. manipolazione di output).*

Il primo tipo di intervento fraudolento menzionato dalla norma in esame ha ad oggetto il funzionamento di un sistema informatico o telematico, e consiste in una modifica del regolare svolgimento del processo di elaborazione e/o trasmissione di dati realizzato da un sistema informatico. Costituiscono un sistema informatico ai sensi della norma in esame anche quegli apparati che forniscono beni o servizi che siano gestiti da un elaboratore: è il caso, ad es., di tutti quegli apparecchi, come macchine per fotocopie, telefoni, distributori automatici di banconote, che funzionano mediante carte magnetiche. Fuoriescono dalla portata della norma incriminatrice quei sistemi informatici che, in sostituzione delle tradizionali serrature, assolvono una funzione di mera protezione (è il caso, ad es., dei congegni elettronici di apertura e chiusura, i quali pure, talvolta, operano attraverso carte magnetiche). Con la formula *"intervento senza diritto su dati, informazioni o programmi"* si è data rilevanza ad ogni forma di interferenza, diretta e indiretta, in un processo di elaborazione di dati, diversa dalla alterazione del funzionamento del sistema informatico. L'intervento sui dati potrà consistere tanto in una alterazione o soppressione di quelli contenuti nel sistema o su un supporto esterno, quanto nella introduzione di dati falsi.

Non può invece ravvisarsi un intervento senza diritto sui dati nel caso di semplice uso non autorizzato dei dati integranti il codice personale di identificazione altrui, con riferimento a quei sistemi informatici che consentono ad una ristretta cerchia di persone di eseguire operazioni patrimonialmente rilevanti, utilizzando un apposito terminale e un codice personale di accesso: è il caso, ad es., del servizio di home banking, attraverso il quale i clienti di una banca possono eseguire una serie di operazioni bancarie, servendosi del terminale situato a casa loro e facendosi riconoscere dal computer attraverso gli estremi del proprio numero di identificazione. L'uso indebito del codice di identificazione altrui, d'altra parte, consente soltanto l'accesso al sistema informatico e non anche, in modo diretto, il conseguimento di un ingiusto profitto; quest'ultimo può eventualmente derivare dal successivo compimento di uno spostamento patrimoniale ingiustificato, attraverso un vero e proprio intervento senza diritto sui dati. Il risultato irregolare del processo di elaborazione manipolato deve avere un immediato risvolto economico, ed essere quindi idoneo ad incidere sfavorevolmente nella sfera patrimoniale altrui: solo a questa condizione, infatti, può dirsi che il danno che la vittima della frode subisce sia

derivato direttamente dagli effetti sfavorevoli prodotti, nella sua sfera patrimoniale, dal risultato alterato del procedimento di elaborazione.

2.2.o) La convenzione di Budapest sul Cybercrime. Aspetti di diritto sostanziale.

Il 18 marzo 2008 il Parlamento italiano, approvando la Legge n. 48, sanciva il pieno ingresso nel nostro ordinamento (autorizzandone appunto la ratifica) della Convenzione sul *"Cybercrime"* varata dal Consiglio d'Europa.
La Convenzione è stata il frutto di parecchi anni di lavoro da parte di un comitato di esperti istituito nel 1996 dal CEPC (Comitato Europeo per i Problemi Criminali). Il testo della Convenzione di Bupadest è stato quindi il punto di arrivo di una comune volontà europea di creare degli efficaci strumenti di lotta al *cybercrime*, armonizzando le norme incriminatrici tra i vari paesi aderenti e prevedendo effettive e rapide forme di collaborazione e cooperazione a livello internazionale.
In tale ottica, va segnalato (come del resto si vedrà *infra*) che la legge 48/08, intervenendo in maniera robusta principalmente sugli aspetti processualpenalistici e sulle forme e procedure di cooperazione internazionale, ha apportato modifiche minimali all'impianto penalistico preesistente.
Così, in tema di *falsità informatiche,* è stato soppresso il secondo periodo del comma 1 dell'art. 491*bis* - quello che stabiliva che per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli. Il legislatore si è infatti reso conto che tale definizione, concepita come avente ad oggetto i supporti anziché i contenuti dichiarativi o probatori trattati con le tecnologie informatiche, creava più problemi di quanti ne risolvesse. Mediante l'abolizione di tale definizione, quindi, si è reso possibile un implicito richiamo alla corretta nozione di documento informatico derivante da molteplici norme a carattere extrapenale: alla stregua delle previsioni contenute nel DPR 513/97, nel Testo Unico della Documentazione Amministrativa (d.p.r. 445/2000) ed nel Codice dell'Amministrazione Digitale (d.l.gs. 82/2005), il documento informatico può essere definito come la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
La legge n°48/08 ha altresì introdotto forme di reato del tutto inedite quali, ad esempio, la *Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri* (art. 495bis). Si tratta di un reato comune, realizzabile da chiunque renda al certificatore dichiarazioni o attestazioni false, ideologicamente o materialmente. Tale disposizione sembra essere diretta a tutelare la firma digitale che, per essere generata, necessita, come noto, di un soggetto "certificatore".
Altra nuova norma è la Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 *quinquies* c.p.). Secondo il legislatore,

l'introduzione di tale fattispecie è risultata indispensabile per coprire alcune condotte tipiche che non sarebbero rientrate nella frode informatica ex art. 640*bis* c.p. .
Seguendo puntuali indicazioni promananti dalla Convenzione di Budapest, il legislatore italiano ha inoltre operato una bipartizione tra *danneggiamenti di dati* e *danneggiamenti di sistemi*.
Un primo intervento di restyling ha riguardato l'art. 615 *quinquies (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico).* Anche in questo caso si è inteso fare riferimento a delle condotte *("si procura, produce, riproduce, importa"*) che risultavano precedentemente escluse dalla fattispecie criminosa. E' stato inoltre introdotto il dolo specifico dell'agente. Simile operazione di ritocco è stata effettuata anche sull'art. 635 *bis* c.p. (*Danneggiamento di informazioni, dati e programmi informatici*). Pure in questo caso la novella ha allargato il novero delle condotte punibili. Da segnalare, inoltre, che ora il primo comma prevede la procedibilità non d'ufficio, ma a querela della persona offesa. Già dalla rubrica risulta la più evidente novità. L'art. 635 *bis* non riguarda più i sistemi informatici e telematici, bensì le informazioni, i dati ed i programmi informatici. I sistemi informatici sono ora puniti in un autonomo e più grave delitto, l'art. 635quater. (Danneggiamento di sistemi informatici o telematici.).
Il nuovo reato contiene una più ampia ed articolata descrizione del fatto tipico. Oltre ad essere realizzabile mediante le condotte indicate nell'art. 635bis, è prevista anche la punibilità di chi introduce o trasmette dati, informazioni o programmi. Tale previsione si è resa necessaria per punire specificamente i danneggiamenti realizzabili anche a distanza mediante *malware* introdotti o fatti circolare in rete. Parallelamente il legislatore ha abrogato i commi 2 e 3 dell'art. 420 c.p., introducendo due nuove figure criminose con gli articoli 635ter (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità) e art. 635 *quinquies* (Danneggiamento di sistemi informatici o telematici di pubblica utilità). Oltre ad avere posizionato i due nuovi articoli nei delitti contro il patrimonio (e non più in quelli contro l'ordine pubblico), la nuova previsione ha separato gli oggetti passivi del reato: informazioni, dati e programmi nell'art. 635 *ter* e i sistemi informatici o telematici nell'art. 635 *quinquies*. Entrambi i reati, poi, presentano in comune l'aggravante dell'effettivo danneggiamento, con una pena edittale che parte da tre anni per arrivare sino a otto anni. Da notare ancora che la protezione garantita ai dati ed ai sistemi di pubblica utilità è più forte rispetto a quella stabilita per i dati ed i sistemi privati.
Merita infine di essere segnalato che la legge 48/08, oltre a modificare ed introdurre nuovi commi e articoli nel codice penale e, soprattutto, di procedura penale – segnatamente (come si vedrà *infra*) in tema di ispezioni, perquisizioni e sequestri - ha

altresì esteso la responsabilità degli enti per gli illeciti da reato anche alle ipotesi di delitti informatici (salvo limitate esclusioni)[115].

2.2.p) Spunti comparatistici in tema di tutela delle comunicazioni telematiche.

Ferme restando le comuni norme di derivazione convenzionale e l'avvicinamento delle legislazioni penali e procedurali dei (tanti) Paesi che hanno dato attuazione all'interno del proprio ordinamento alle disposizioni contenute nella Convenzione di Budapest, per quanto attiene invece alla tutela delle comunicazioni informatiche e telematiche *tout court*, i legislatori di altri importanti Paesi europei sembrano aver preferito una strada diversa, rispetto a quella percorsa dal nostro Parlamento. Nel Codice penale tedesco[116], ad es. - nel quale non esiste un delitto "generale" d'indiscrezione, ma in cui viene punita la violazione della *riservatezza verbale* (§201), del *segreto epistolare* (§202), o di quello *professionale* (§203) - le comunicazioni telematiche (più che informatiche) rientrano nel più ampio concetto di *"comunicazioni a distanza"*, la cui segretezza è tutelata dalla fattispecie incriminatrice cui al §206 (Violazione di segreto postale o relativo ad altre forme di comunicazione a distanza); la segretezza, però, si ritiene violata solo quando i fatti di cui il soggetto attivo sia venuto a conoscenza, a seguito di un'attività di intercettazione autorizzata (o non autorizzata), siano rivelati a terzi. È importante segnalare, inoltre, che, sempre secondo il citato paragrafo, sono considerati coperti da segreto anche i c.d. dati esterni alle comunicazioni.

Anche in Spagna, poi, le comunicazioni telematiche sono tutelate perché rientrano nel concetto generale di "altro segnale di comunicazione", di cui all'art. 197 c.p.[117]. Articolo che prevede un vero e proprio delitto "generale" d'indiscrezione, nell'ambito del quale le condotte tipiche sono punite in quanto finalizzate a "scoprire segreti o violare l'intimità di altri". A proposito della normativa spagnola, bisogna sottolineare che la divulgazione del segreto, diversamente da quanto avviene in Italia, non pare costituire un delitto autonomo, ma una circostanza aggravante. Pure la circostanza che il soggetto attivo sia un pubblico ufficiale, che abbia approfittato del suo incarico per commettere il delitto, comporta un aumento di pena. È singolare, tuttavia, che qualora il p.u. abbia agito "al fine di perseguire un delitto" il fatto divenga costitutivo di un altro reato, e cioè di quello previsto dall'art. 535 c.p., che fa parte dei delitti contro la Costituzione (Titolo XXI), e non contro la riservatezza (Titolo X), ed è

---

[115] Va ricordato che il d.l.gs 231/2001 ha introdotto nel nostro ordinamento la responsabilità degli enti (enti forniti di personalità giuridica, società e associazioni anche prive di personalità giuridica) per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

[116] Cfr. Il Codice penale tedesco, a cura di Vinciguerra, intr. H.H. Jeschek, trad. Donadio-Cornacchia-DeSimone-Foffani-Fornasari-Mangels-Sforzi-Summerer, Padova, II ed., 2003.

[117] Il Codice penale spagnolo, intr. Quintero Olivvares, trad. Naronte, Padova, 2007.

sanzionato in modo assai più blando, e comunque solo con pene interdittive. Al contrario, nel nostro ordinamento, la qualità di p.u. del soggetto attivo comporta sempre un aggravamento di pena, a prescindere dalla circostanza che questo agisca, illecitamente, per fini investigativi o personali. Comunque sia, anche senza che vi sia bisogno di scendere ulteriormente nel dettaglio delle singole normative straniere, quel che si ritiene importante segnalare è che, la medesima condivisibile tendenza a tutelare le comunicazioni telematiche, all'interno di una protezione più generale delle telecomunicazioni tra persone - e non, come in Italia, fra sistemi - , si riscontra anche nel Codice penale francese (art. 226-15)[118], ed in quello portoghese (art. 194). Desta davvero preoccupazione, invece, la sottile distinzione operata recentemente dalla giurisprudenza statunitense[119], tra *"wire communications"* ed *"elettronic communications"* - quest'ultime dotate di una protezione minore - per negare che costituisca delitto l'illecita presa di cognizione di e-mail altrui - per altro compiuta, sistematicamente, da una società commerciale, per fini di lucro - specie se si considera che tale decisione è maturata in un contesto in cui, da una parte, l'opinione pubblica, dopo gli attentati alle Twin Towers ed al Pentagono[120], pare ormai convinta che la limitazione delle c.d. libertà civili costituisca un prezzo equo per ottenere maggiore sicurezza sociale e, dall'altra, il *Patriot Act* e *l'Homeland Security Act* hanno ridisegnato, ampliandolo significativamente, l'ambito del controllo legale sulle comunicazioni telematiche[121]. Ambito che prima era disciplinato dal *Control and Safe Streets Act,* del '68, per le questioni interne, e dal *Foreign Intelligence Surveillance Act*, del '78 - nel quale, tuttavia, già emergeva una certa tendenza all'erosione delle garanzie - per le indagini inerenti ai c.d. "*foreign powers*" (Stati stranieri e loro istituzioni, gruppi ed enti composti o comunque controllati, prevalentemente, da cittadini non statunitensi, ecc.).

2.3 La *"digital evidence".*

2.3.a) Premessa.

L'importanza che la prova scientifica, generalmente intesa, riveste oggi nel processo è di tutta evidenza.

Le ragioni sono facili da rinvenire nel bisogno di certezza insito in ogni giudizio di responsabilità ed in modo particolare in quello penale.

---

[118] www.legifrance.gouv.fr.

[119] Cfr.Corte Federale d'Appello U.S., 29 giugno 2004, in Foro it., 2004, IV, 449 ss., con nota di Di Ciommo.

[120] Manna, *Erosione delle garanzie individuali in nome dell'efficienza dell'azione di contrasto al terrorismo: la privacy*, in Riv. it. dir. proc. pen., 2004, 1022.

[121] *Rebecca, Intelligence e controllo delle comunicazioni telematiche nella legislazione statunitense antiterrorismo,* in Dir. pen. proc., 2003, 1292 ss.

La prova scientifica (dai tradizionali esami medico-legali e balistici alle più recenti analisi chimiche, biologiche, tossicologiche fino all'analisi del DNA e delle *tracce elettroniche*) viene dunque sempre più privilegiata rispetto alla prova dichiarativa e ciò dipende indubbiamente dal diverso valore probante delle due[122].

Si pensi, a titolo esemplificativo, che il riconoscimento effettuato mediante ricognizione personale ha un margine di errore del 4%, mentre l'identificazione a mezzo del profilo genetico con l'utilizzo di 10 STR[123] contempla un margine di errore di 1/1 Mld.

L'ordine di grandezza dell'errore scientifico è dunque talmente piccolo, se paragonato all'errore umano, da potersi praticamente fregiare di un connotato di quasi certezza tale da indurre il legislatore a ricorrere sempre più spesso a siffatta opzione probatoria.

Tuttavia, il rapporto scienza e processo è estremamente delicato, per ragioni metodologiche, ma anche per l'impossibilità della legge processuale di recepire la legge scientifica *tout court*.

Quanto al metodo, scienza e processo sono in antitesi: mentre la prima procede per *metodo induttivo* fondato su esperimenti empirici e la sua evoluzione è data da assunti (e dal progressivo superamento degli stessi) basati su errore, dubbio e dialettica, il processo è un *metodo deduttivo*, prettamente autoritario (autorità della legge e del giudice che la applica) che impone soluzioni univoche, immutabili ed insindacabili e in cui il dubbio e l'errore sono elementi disturbanti da estirpare (basti pensare al concetto dell' *"al di là di ogni ragionevole dubbio"* sancito dall'art. 533 c.p.p).

In ordine invece al recepimento della scienza nel processo, la legge non può per definizione né fissarne il contenuto epistemologico, né codificarla in protocolli predefiniti. Del resto, se così non fosse, si tornerebbe all'equazione prova scientifica = prova legale, principio che nell'odierno contesto processuale è assolutamente improponibile.

Per di più, il principio della libertà della prova in materia penale consente, d'altra parte, l'ingresso nel processo di prove tecnico-scientifiche sempre nuove e innovative.

Diventa, tuttavia, dirimente, a garanzia del diritto di difesa, la *modalità* con cui la prova viene acquisita, specie laddove il contenuto della prova in sé è talmente tecnico che non lascia spazio ad argomentazioni difensive di merito.

---

[122] In questo senso cfr. Dominioni, *La prova penale scientifica*, Giuffrè 2005.

[123] Si definiscono microsatelliti (o short tandem repeats o STR) sequenze ripetute di DNA non codificante costituite da unità di ripetizione molto corte (1-5 bp) disposte secondo una ripetizione in tandem, utilizzabili come marcatori molecolari. I microsatelliti presentano un alto livello di polimorfismo e sono marcatori informativi negli studi di genetica di popolazione comprendenti approfondimenti dal livello individuale a quello di specie strettamente affini. Infatti, grazie allo studio dei microsatelliti, è possibile creare un profilo del DNA (DNA profiling o impronta genetica) grazie al quale individuare un individuo. Il confronto genetico potrà essere effettuato confrontando la diversa lunghezza dei microsatelliti presenti in individui differenti. Tali differenze caratterizzano il polimorfismo di ripetizione.

All'interno del *genus* prova scientifica, inoltre, la *prova informatica* rappresenta una sottospecie connotata da ulteriori peculiarità che schiudono, a loro volta, ulteriori e controbattute questioni giuridiche.
La prova informatica o elettronica (*la c.d. digital evidence*) è infatti connotata da due caratteristiche: *fragilità* e *immaterialità*. Le tracce elettroniche sono fragili in quanto facilmente alterabili, danneggiabili e distruttibili. La fragilità della traccia elettronica è congenita ed intrinseca; prescinde dunque da ipotetiche manipolazioni dolose ma sin anche da eventuali comportamenti colposi posti in essere da chi interviene su di esse. La perdita casuale di dati è infatti talmente frequente da porsi come problema cogente che necessita di soluzioni *ad hoc* (la sola accensione di un computer spento o l'apertura di un *file* comporta infatti l'aggiornamento automatico dell'orario di accesso compromettendo quello precedente, così come il mancato utilizzo di uno specifico *text editor* nella fase di copiatura può compromettere la genuinità del testo originario).

2.3.b) La *computer-generated evidence (CGE)* [e la computer-derived evidence *(CDE)]*[124].

All'interno dell' ampia categoria della *"digital evidence"* si possono distinguere, da un lato, la c.d. *computer generated evidence (CGE)*, e, dall'altro, la *computer-derived evidence(CDE)*.
La *computer-generated evidence* fa capo alle ipotesi in cui lo strumento informatico viene convenientemente utilizzato ai fini della dimostrazione delle modalità di accadimento di un fatto mediante la sua rappresentazione virtuale. Il percorso di ricostruzione fattuale è scandito in sei fasi che, a partire dalla raccolta delle evidenze disponibili e rilevanti alla definizione delle modalità di accadimento del fatto storico, giunge, attraverso l'analisi dei dati inseriti nel computer (elaborati mediante software *ad hoc*), alla realizzazione di un filmato che illustra la dinamica di svolgimento del fatto o dei fatti.
L'impiego di questa tecnologia in sede processuale può essere ricondotta a due diverse finalità. *In primis*, ci si può limitare alla elaborazione mediante PC di una serie di immagini o suoni che fungano da sussidio visivo alla relazione dell'esperto. In questo caso, il computer costituisce mero ausilio illustrativo di un diverso mezzo di prova, di cui mira ad accrescerne l'efficacia dimostrativa (cd. animazione)[125]. *In secundis*, il computer può essere utilizzato al fine di rappresentare l'evento per dimostrarne le circostanze reali di accadimento (c.d. ricostruzione) o di simulare la verificazione della medesima condotta in circostanze diverse da quelle che si assumono realizzate al fine

[124] Il distinguo è prospettato da L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica,* cit., p. 145.
[125] L'utilizzo dello strumento del computer in funzione ausiliare della relazione dell'esperto è avvenuta, nel nostro ordinamento, ad es. nel corso del procedimento Cusani e in quello per la strage di Capaci.

dimostrare in via ipotetica, ad esempio, che l'evento non si sarebbe realizzato in condizioni diverse (cd. simulazione)[126].

Fondandosi sul tratto discretivo della funzione ancillare rispetto all'operato dell'esperto, nel caso dell'*animazione*, e, all'opposto, della piena autonomia probatoria della rappresentazione virtuale, nei casi della *ricostruzione* e della *simulazione*, tale classificazione consente, per un verso, di ricondurre la prima ipotesi nell'alveo della prova peritale, di cui costituisce uno strumento tecnico impiegato al fine di potenziare l'efficacia probatoria delle conclusioni redatte dall'esperto; ed impone, per altro verso, di qualificare la *ricostruzione* e la *simulazione* sub specie dell'esperimento giudiziale ex art. 216 c.p.p., in qualità di particolari modalità tecnico-scientifiche di svolgimento delle operazioni sotto la guida dell'esperto designato dal giudice.

La sistemazione dogmatica appena prospettata appare rispettosa della elaborazione giurisprudenziale sedimentata in tema di individuazione dei tratti distintivi tra esperimento e prova peritale[127], esaltandone, in entrambi i casi, le potenzialità cognitive.

A questo punto, occorre spendere alcune considerazioni in merito alla riconduzione della *ricostruzione* e della *simulazione* nel novero delle modalità di svolgimento dell'*esperimento giudiziale*. Da un lato, essa appare in linea con il dato testuale dell'art. 219 c.p.p., che contiene un elenco di natura meramente esemplificativa, desumibile dalla clausola di apertura dell'art. 219 comma 2 c.p.p., degli strumenti utilizzabili per l'esecuzione delle operazioni che si rendano di volta in volta necessarie.

Dall'altro lato, l'inciso di cui all'art. 218 c.p.p. che individua l'oggetto della prova sperimentale nella riproduzione delle modalità di svolgimento della *res giudicanda "per quanto è possibile"*, pare sottendere la necessità di addivenire ad un giudizio, scandito secondo le consuete soglie di progressività crescente in relazione alla fase del procedimento probatorio, di idoneità del mezzo di prova in riferimento alle specifiche caratteristiche del fatto concreto.

Per cui, da un lato, il fatto deve essere suscettibile di riproduzione, e, dall'altro, il mezzo di prova prescelto deve possedere un'attitudine dimostrativa circa la possibilità di verificazione della *res giudicanda*.

La valutazione di idoneità probatoria è resa problematica, nel caso di specie, dalla complessità della tecnica impiegata, in relazione alla quale la parte che ne richiede l'acquisizione avrà tutto l'interesse a fornire al giudice gli strumenti di valutazione che lo conducano ad un giudizio positivo circa l'attendibilità della tecnica probatoria.

A tal fine, essa potrà ricorrere ad una valutazione mediante esperto - sui profili della sufficienza dei dati trasmessi al *software*, dell'attendibilità e della verificabilità del

---

[126] Tale metodo ricostruttivo, nella forma della simulazione, è stato utilizzato ad es. nel caso del processo penale per la morte del pilota Ayrton Senna svoltosi a Imola nel 1997 contro la squadra Automobilistica Williams. Nel caso di specie, il giudice ha ritenuto che la prova non potesse essere ammissibile in relazione al carattere sperimentale del metodo ed alla mancanza di un adeguato corredo di protocolli d'uso che consentisse di testarne l'affidabilità. Così, Corte App. Bologna, sez. III, 22 novembre 1999, Williams e altri, inedita, p. 112.

[127] Ex plurimis: Cass., sez. V, 28 novembre 1997, Angioi, in Guida dir., 1998, f. 13, p. 92; Cass., sez. VI, 19 gennaio 1996, Pezzatini, in C.E.D. Cass., n. 204149; Cass., sez. II, 27 gennaio 1995, Amico, in Giust. pen., 1995, III, c. 728.

funzionamento del programma informatico - da fare acquisire al processo nelle forme della consulenza o della perizia, evidenziandosi, per questa via, un rapporto di reciprocità tra i due mezzi, fruibili l'uno in funzione ausiliaria rispetto all'altro[128].

2.3.c) La computer-derived evidence *(CDE).*

La computer-derived evidence fa capo invece alle ipotesi in cui il dato digitale estrapolato dall'elaboratore costituisce prova, diretta o indiretta, di un elemento costitutivo della *res giudicanda*.

La dottrina, come si accennava nel para. 2.3.a), ha ripetutamente messo in luce le peculiarità che distinguono la *digital evidence* rispetto alla prova cd. "fisica", individuandole essenzialmente nella *immaterialità del dato* e nella sua conseguente *facile alterabilità*[129].

Il dato informatico è costituito da una sequenza binaria composta da 0 e 1 e resa intelligibile a seguito dell'elaborazione di un processore mediante codice ASCII[130] o altra codifica[131]. Tale caratteristica strutturale vale a dar conto della immaterialità dell'incorporamento digitale, che opera in una duplice direzione.

Da un lato, l'intelligibilità del dato dipende dalla codificazione dell'elaboratore che ne opera la rappresentazione. Dall'altro lato, la rappresentazione del dato prescinde dal supporto fisico su cui il dato è incorporato. Di conseguenza, il dato si rivela autonomo rispetto alla base fisica su cui viene memorizzato di volta in volta, e, pertanto, può essere facilmente trasferito da un supporto all'altro.

Censurando l'inadeguatezza della definizione legislativa di documento informatico vigente a seguito della novella n. 48 del 2008, che, mediante l'abrogazione dell'art. 491 bis secondo periodo c.p., ha determinato la reviviscenza della coeva definizione contenuta nel codice dell'amministrazione digitale del 2008 incentrata sul concetto di rappresentazione (su cui cfr. *supra* para 2.2.O), la dottrina ha chiarito che è proprio la particolarità del metodo di incorporamento a costituire la nota distintiva tra le prove digitali e le prove reali tradizionali. Mentre queste sono incorporate attraverso il metodo analogico, per cui la rappresentazione sul supporto fisico è, per così dire, immediata ed esiste solo a condizione e nelle modalità impresse sul supporto, quelle sono incorporate con metodo digitale, per cui la rappresentazione è mediata dall'elaborazione del processore e fa capo ad uno o più supporti fisici, contraddistinti da un elevato grado di alterabilità e modificabilità senza che rimanga alcuna traccia –

---

[128] Ravvisa un rapporto di fungibilità tra esperimento e perizia, A. MELCHIONDA, in E. MARZADURI *Giurisprudenza sistematica di diritto processuale penale,* dir. da M. Chiavario-E. Marzaduri, Torino, 1999

[129] Così, S. ATERNO in, *Acquisizione e analisi della prova informatica*, in Dir. pen. proc., 2008, Suppl. Dossier.

[130] ASCII è l'acronimo di American Standard Code for Information Interchange (ovvero Codice Standard Americano per lo Scambio di Informazioni), definizione tratta dal sito *www.amolamatematica.it*.

[131] La codifica in questione è una convenzione che associa ad ogni precisa successione (ad 8 cifre, cioè 1 byte) di 0 e 1 un simbolo. Così, S. ATERNO, *Acquisizione e analisi della prova informatica*, op. cit p. 62

si considerino, a titolo esemplificativo, l'hard disk, il cd, la pendrive, fino ai moderni dispositivi basati su memorie *flash* – che non la condizionano in alcun modo, anche se per l'esistenza fisica del dato è necessaria la sua memorizzazione su almeno un supporto.
Corollario della volatilità ed alterabilità ontologica del dato informatico è la necessità di delineare, ai fini della sua utilizzabilità in ambito forense, un *procedimento acquisitivo* che preservi e garantisca la genuinità del dato, sotto il duplice profilo della autenticità e della integrità del medesimo[132].
Il percorso che dalla identificazione del dato rilevante giunge alla sua presentazione in giudizio assume le forme di un procedimento "*step by step"* che deve essere in grado di garantire la *genuinità del dato*, valendosi di strumenti operativi (c.d. *tools*) che ne impediscano l'alterazione e il deterioramento, e di assicurare la *tracciabilità* di ogni momento della catena procedimentale (*c.d. chain of custody*) in funzione della verificabilità della correttezza delle operazioni da parte del giudice e delle parti processuali.
Proprio al fine di garantire il massimo ossequio, ai fini probatori, alle cennate precondizioni di utilizzabilità in ambito processuale del dato "derivato" da un' "elaborazione" informatica (o, più estesamente, digitale), si sono andate stratificando negli anni – condensate in articolate massime giurisprudenziali – tutta una lunga serie di prassi e pratiche tecnico-giudiziali volte ad assicurare, attraverso il conveniente uso di specifici software, un adeguato impiego ed una sicura metodologia di estrazione informatica dei dati contenuti nelle memorie e nei supporti di archiviazione degli elaboratori digitali.
Ed è a questa pratica - inizialmente empirica ma che col passare degli anni è andata progressivamente assumendo vera e propria dignità di scienza - che ci si vuol in concreto riferire allorquando si adopera l'astrusa espressione inglese *"computer forensics"*.

2.3.d) La c.d. computer forensic.

In termini estremamente sintetici e generali, per *computer forensics* si intende *"…quella scienza che studia il valore che un dato correlato a un sistema informatico o telematico può avere in ambito giuridico, o legale che dir si voglia"*[133]. Conseguentemente detta disciplina si occupa della preservazione, dell'identificazione, dello studio e della documentazione dei computer, o dei sistemi informativi in generale, al fine di evidenziare l'esistenza di prove nello svolgimento dell'attività investigativa. La sua vocazione naturale, quindi, è di presentarsi quale

[132] Così, L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica*, op. cit., p.147.
[133] P. Perri, La computer forensics, in *Manuale breve di informatica giuridica*, a cura di G. Ziccardi, Milano, 2006.

vera e propria branca del sapere scientifico[134] - e al tempo stesso giuridico - preordinata all'acquisizione, all'analisi ed all'esposizione in sede processuale (e con linguaggio giuridico) di ogni genere d'informazione "probatoria" memorizzata o trasmessa in formato binario (*alias* digitale).

Ciò che pertanto viene chiesto all'esperto di *computer forensics* (perito o consulente che sia) è di acquisire le prove senza alterare o modificare il sistema informatico su cui si trovano. Garantire quindi che le prove, acquisite su altro supporto "di massa", siano identiche a quelle originarie; analizzare i dati avendo cura che l'attività di "discettamento" (*screening probatorio*) non alteri, modifichi o corrompa le risultanze digitali utili ai fini probatori.

Per sua stessa definizione la *computer forensics* è una disciplina estremamente duttile e potenzialmente adattabile ad ogni ritrovato della tecnica che sfrutti, direttamente o indirettamente, le acquisizioni della tecnologia digitale per implementare il suo funzionamento: quindi innanzitutto elaboratori digitali, ma non soltanto: reti internet e router; dispositivi cellulari, PDA ed in generale ogni dispositivo a carattere "mobile". Presenta quindi una geometria variabile, suscettibile di rifrangersi in molteplici *sub categorie* quanti sono gli apparati tecnologici di nuova generazione che vengono alla luce nel quadro dell'evoluzione, sempre crescente, delle tecnologie informatiche e digitali.

Più specificatamente, in ragione della sua fonte o ambito di applicazione essa, pertanto, si sostanzia nella *network forensic* – che ha ad oggetto i dati ricavabili dalle comunicazioni in rete – nella *mobile forensic* – che riguarda l'impiego dei dispositivi mobili – e nella *digital forensic*, riservata allo studio del dato digitale quale che ne sia la fonte.

Tale precisazione terminologica è essenziale in quanto consente di individuare i confini esterni della disciplina in trattazione, che si limita unicamente a considerare l'apprensione, l'analisi e la presentazione in giudizio dei dati digitali rinvenibili dalla fonte statica dell'elaboratore senza, peraltro, estendersi alla materia dinamica delle tecnologie di *networking*, aventi ad oggetto i dati ricavabili dalle comunicazioni in rete (che afferiscono specificatamente all'ambito applicativo delle intercettazioni telematiche ed informatiche disciplinate dall'art. 266 bis c.p.p.).

Come si è accennato in precedenza, il punto più delicato, tra tutte le questioni attinenti alla *computer forensics*, riguarda proprio la sua attagliabilità alle regole e alle esigenze peculiari del processo penale. Negli ultimi decenni, infatti, l'accertamento penale si è lentamente arricchito di inediti contenuti scientifici e di apporti tecnologici di sempre maggiore complessità ed incisività.

Peraltro, nell'ambito della nostra prassi giudiziale, solo con grave ritardo si è iniziato ad avvertire l'enorme e fortissimo impatto che il proliferare della c.d. *scientific evidence* ha sortito sul processo penale; circostanza, quest'ultima, che ha addirittura indotto ad interrogarsi circa il fatto se abbia ancora senso parlare della prova orale in termini di chiave di volta del processo accusatorio, allorché sempre più giudizi paiono

[134] Nel 1992, la disciplina in parola venne battezzata come categoria autonoma nel noto saggio di Collier e Spaul apparso sul *Journal of forensic science.*

fondarsi su evidenze scientifiche formatesi prevalentemente nella prima fase del procedimento (quella appunto delle indagini preliminari) e che, veicolate nella scansione dibattimentale, riducono il "contraddittorio per la prova" ad un mero esercizio di dialettica su materiali non facilmente decifrabili e già "preconfezionati" in sede appunto di indagini preliminari[135].

Le indagini informatiche prodromiche alla presentazione del dato digitale in giudizio, in particolare, si compongono di una prima fase, volta all'*individuazione e all'acquisizione* materiale del dato, cui segue la seconda fase, finalizzata all'*analisi* del dato in appositi laboratori informatici. Il punto centrale della fase acquisitiva è costituito, in ottemperanza alle *guidelines* operative vigenti in *subiecta materia*, dalla creazione di una copia-clone dei supporti formata mediante codici hash[136]. La tecnica hashing garantisce la conformità assoluta della copia all'originale, e, allo stesso tempo, consente agli operatori di manipolare i dati senza rischi di alterazione degli stessi. Tra l'altro, operando in tal modo, è possibile effettuare la clonazione dell'*hard disk* senza che si renda necessario il sequestro del processore, che può pertanto rimanere nella disponibilità dell'operatore.

Tali conclusioni parrebbero legittimare, a prima vista, l'inclusione delle operazione *de quibus* nel novero dei rilievi ed accertamenti urgenti di p.g. ex art. 354 comma 2 c.p.p. Con lo specificare che l'operatore di p.g. deve limitarsi ad assicurare la conservazione e ad impedire l'alterazione dei sistemi informatici, provvedendo, ove possibile, *"alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità"*, in effetti, il legislatore parrebbe riferirsi proprio a tali attività. Sennonché, come è stato acutamente rilevato in dottrina[137], tali operazioni conservano sempre, in realtà, un margine intrinseco di rischio di alterazione dei dati, soprattutto ove si consideri che la creazione della copia clone *(c.d. bitstream image)* avviene mediante l'utilizzo di *tools* coperti da licenza, e, pertanto, retti da meccanismi di funzionamento non accessibili, e, pertanto, non verificabili, dal giudice

---

[135] In questi termini Luparia, *Processo penale e tecnologia informatica* in Diritto dell'internet, n°3 del 2008, 221 ss.

[136] Hash è un termine della lingua inglese (*to hash* sminuzzare, pasticciare). Gli algoritmi di hash, in particolare SHA1 e MD5, sono largamente utilizzati nell'ambito dell'informatica forense per validare e in qualche modo "firmare" digitalmente i dati acquisiti, tipicamente le copie forensi. La recente legislazione impone infatti una catena di custodia che permetta di preservare i reperti informatici da eventuali modifiche successive all'acquisizione: tramite i codici hash è possibile in ogni momento verificare che quanto repertato sia rimasto immutato nel tempo. Tratto dal sito: www.wikipedia.org: l'operazione di hashing serve, quindi, a generare una sorta di marchio digitale o impronta che contraddistingue univocamente il dato informatico e ne garantisce l'integrità; consiste nell'applicazione di un formula matematica (algoritmo del tipo "funzione di hash") al supporto originale e alla copia: i valori dei due calcoli coincidono solo se vi è assoluta rispondenza tra l'originale e la copia.
Va peraltro segnalato che già da alcuni anni la piattaforma comunemente usata per il calcolo dell'hash, l'MD5, è stata dimostrata inaffidabile da un gruppo di scienziati cinesi per la possibilità di c.d. "collisioni".

[137] Così, L. LUPARIA, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*. Legge 18 marzo 2008, n. 48, in Dir. pen. proc., 2008, p. 720.

e dalle parti processuali in sede di presentazione[138]. In tale prospettiva, sarebbe stato preferibile ricorrere allo strumento degli accertamenti tecnici irripetibili al fine di garantire il diritto di difesa, e, soprattutto, di assicurare il contraddittorio fin dalla prima fase di trattamento del dato digitale[139].

All'acquisizione della fonte di prova informatica mediante copia-clone, segue, come si diceva *supra*, la fase tecnica dell'analisi dei dati finalizzata al recupero delle informazioni rilevanti in sede processuale, anche mediante lettura di *files* cancellati o residuati *nell'hard disk* o l'analisi dei *files di log* che consentono di ricostruire sequenze di operazioni e di ricondurle ai loro autori. Anche in questa sede è di estrema importanza per la genuinità del risultato probatorio che gli operatori – i quali, in base alle *guidelines operative*, dovrebbero lavorare in laboratori certificati ISO – procedano mediante *tools* che preservino il dato da possibili alterazioni e garantiscano la riproducibilità delle operazioni mediante la registrazione di tutte le attività eseguite in un *log* o in un *report* (*cd. Logging* delle attvità)[140]. Si noti che la ripetibilità delle operazioni svolte è importante, nella prospettiva di una successiva relazione peritale da presentare in dibattimento, al fine consentire al giudice e alle parti la verifica di ogni *step* della *chain custody*.

Quanto all'ingresso della prova informatica in sede processuale, la caratteristica della ripetibilità delle operazione di analisi una volta realizzata la *bitstream image* condurrebbe a ritenere che, creato il disco clone con la procedura degli accertamenti irripetibili, sia possibile eseguire su di esso una serie di accertamenti ripetibili mediante la consulenza tecnica ex art. 359 c.p.p., in indagini preliminari, e la perizia in sede dibattimentale. In alternativa, è prospettabile la riconducibilità delle attività tecnica di clonazione del supporto e delle analisi in laboratorio nella cornice delineata dall'art. 360 c.p.p., con la duplice conseguenza del riconoscimento del diritto della difesa di sollecitare il ricorso alle forme dell'incidente probatorio[141], e dell'inclusione dei risultati della prova informatica nel fascicolo dibattimentale.

Ad ogni modo, in base all'opinione prevalente, l'individuazione della *perizia* e della *consulenza tecnica* – declinabile nella forma della consulenza endoperitale, quando si inserisca nell'ambito di un accertamento peritale disposto dal giudice, ed

---

[138] Per tale rilievo, L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica,* cit., p. 153.

[139] Ante riforma, la soluzione *de qua* era stata auspicata da S. ATERNO, *Acquisizione e analisi della prova informatica, cit., p. 68.* Per una critica alle scelte legislative post riforma, si veda L. LUPARIA, *La ratifica della Convenzione Cybercrime, cit., p. 720.* Contro questa impostazione, peraltro, si schierano recisamente numerose sentenze della Corte di Cassazione. *Ex plurimiis,* la Sent. del 2 aprile 2009 n. 14511 - Pres. Canzio - Rel. Cassano, in base alla quale *"…non rientra nel novero degli atti irripetibili l'attività di estrazione di copia di file da un computer oggetto di sequestro, dal momento che essa non comporta alcuna attività di carattere valutativo su base tecnico-scientifica, né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità d'informazioni identiche a quelle contenute nell'originale".*

[140] L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica*, cit., p. 153.

[141] Nella prassi, tuttavia, la giurisprudenza di merito è orientata verso il diniego della domanda della difesa volta all'instaurazione dell'incidente probatorio. A tal proposito, si consideri che, a differenza della prova del Dna, il ricorso all'istituto *de quo* è ancorato alla sussistenza dei presupposti ordinari di ammissibilità. Sul punto, anche per i riferimenti giurisprudenziali, si vedano G. CASSANO-I. P. CIMINO, *Diritto dell'internet e delle nuove tecnologie telematiche, Padova, 2009, p. 636*.

extraperitale, se venga disposta in assenza di perizia – quali veicoli di ingresso nel processo penale della prova informatica, risponde all'esigenza di ricondurre le nuove tecniche di accertamento ai principi di oralità e del contraddittorio; principi che, nella formazione della prova, costituiscono l'asse portante di tutta l'architettura del sistema processuale.
Concludendo, si ponga infine mente sulla circostanza che la vera particolarità di tale fenomeno consiste non soltanto nella necessità di individuare nuovi istituti dogmatici cui affidare l'apprensione del dato digitale (cosa che si riscontra anche nell'ambito della fattispecie delle intercettazioni telematiche), ma altresì nella cernita e nella selezione delle strumentazioni più idonee (nella perenne evoluzione e perfezionamento delle stesse), al compimento di tali operazioni. Lo studio dell'accertamento informatico deve dunque necessariamente essere condotto su due distinti piani: quello della congruità dei nuovi mezzi di prova rispetto ai valori fondamentali dell'ordinamento giuridico e quello della idoneità delle singole attrezzature e dei singoli protocolli applicativi a garantire i diritti della difesa e l'attendibilità dell'accertamento penale. Sta in questa duplice prospettiva la difficoltà nell'affrontare un tema che, come detto, già di per sé possiede, specie in punto di esatta precisazione del concetto di "prova digitale", una forte carica di nebulosità teorica.

2.3.e) Le perquisizioni *online.*

Le cc.dd. perquisizioni *online* (od elettroniche) costituiscono uno strumento di indagine nuovo. Non particolarmente meditate nell'ambito del panorama dottrinario e giurisprudenziale italiano, esse si sono trovate invece di recente al centro di un acceso dibattito nell'ordinamento tedesco, in conseguenza di una importante pronuncia del *Bundesverfassungsgericht* (Corte Costituzionale Federale) emessa nel febbraio del 2008 sulla c.d. *Online Durchsuchung.*
Dal punto di vista tecnico, le perquisizioni *online* consentono di estrapolare copie, parziali o totali, delle unità di memoria, fisse o volatili, del sistema informatico posto sotto osservazione (*online search* o *one-time copy*); di rilevare e registrare nel tempo quali siti web vengono visitati, attraverso quele sistema od attraverso quali particolari account che si riferiscono ad un dato sistema (*online surveillance);* al limite, di decifrare quel che viene digitato sulla tastiera collegata al sistema stesso. Ciò per lo più si verifica in due modi: inserendo, nel sistema informatico da "investigare", un programma *ad hoc*, che sia in grado appunto di captare i dati sopra descritti e di trasmetterli, in tempo reale o ad intervalli prestabiliti, agli organi inquirenti, oppure leggendo tali dati durante la loro trasmissione tramite uno *sniffer*[142], secondo un'ampia gamma di possibilità tecniche, dipendenti dagli scopi

[142] Si tratta di un software – noto anche come "analizzatore di rete" - che consente di captare i dati elettronici digitati nel momento stesso in cui vengono inseriti. Appartengono a questa categoria i keylogger (vedi paragrafo 2.2.e) *supra*).

dell'indagine e dalla sofisticatezza tecnica del "programma spia" che viene inserito nel sistema ospite o dello *sniffer*. Il tutto avviene ovviamente all'insaputa dell'utilizzatore del sistema, che si presume sia appunto l'indagato[143].

Le perquisizioni elettroniche, come tutti gli atti a sorpresa, dovrebbero interessare essenzialmente la fase delle indagini preliminari, e più precisamente, intervenire nel momento in cui il soggetto nei cui confronti si procede non è ancora a conoscenza della propria qualità e neppure sospetta di essere posto sotto osservazione.

Da un punto di vista oggettivo, bersaglio delle investigazioni in discorso, come si accennava poc'anzi, sono uno o più sistemi informatici: nulla potendo le perquisizioni *online* dire, di per sé, circa l'identità della persona che in quel momento lo (o li) sta utilizzando, si tratti o meno cioè della persona indagata. Il problema, già postosi nella prassi[144], è risolto caso per caso alla luce di tutte le risultanze in concreto disponibili.

In base all'orientamento giurisprudenziale prevalente, anche le perquisizioni *online*, al pari di ogni altra strumento di ricerca della prova non possono, per loro stessa natura, costituire il primo atto investigativo nell'ambito di un procedimento penale.

Essendo infatti preordinate ad arricchire il corredo probatorio di nuovi e più illuminanti elementi di valutazione e/o dimostrazione, di regola, in uno Stato di diritto, si esclude che le stesse possano essere impiegate quali facile espediente per il procacciamento di nuove notizie di reato. Tuttavia, se si pone mente al duplice profilo operativo riferibile a queste particolari forme di perquisizione (*one time copy – online surveillance)* ci si rende agevolmente conto di quanto le stesse siano dotate di una spiccata attitudine preventiva o, se si vuole, proattiva rispetto a reati ancora ignoti.

Al pari della c.d. localizzazione mediante GPS (su cui *infra*) o di altre forme investigative "digitali" ampiamente utilizzate nella prassi, anche le perquisizioni *online* possono essere ricondotte al *c.d. principio di atipicità delle indagini preliminari* in base al quale gli organi inquirenti possono porre in essere anche atti non specificamente previsti da alcuna norma di legge (purché ovviamente non siano apertamente *contra legem*). Ed in questo senso, le perquisizioni *online* sono da considerarsi veri e propri atti atipici. D'altra parte, non sono sicuramente riconducibili alla categoria delle perquisizioni (c.d tipiche) ex art. 247 e ss. c.p.p.. Le perquisizioni *nominate*, infatti, possono essere unicamente personali o locali e sono strutturalmente orientate alla ricerca del corpo del reato e/o delle cose pertinenti al reato che in caso di reperimento, vengono senz'altro sequestrate; le perquisizioni *online*, invece, si svolgono per lo più in quel luogo virtuale che è il web. Possono prescindere dalla ricerca del corpo del reato e/o delle cose pertinenti al reato e non sfociano necessariamente in un sequestro. Ancora, le perquisizioni tradizionali sono si atti a sorpresa, nel senso che non deve essere dato previo avviso del loro compimento all'indagato, ma quest'ultimo, ove presente, ben si accorge, durante lo

[143] Va da se che un dato sistema informatico o telematico possa essere utilizzato da più soggetti anche mediante il medesimo account (c.d. uso promiscuo).

[144] Il fenomeno è molto diffuso nell'ambito delle attività di indagine di contrasto alla pedopornografia poste in essere ai sensi delle previsioni contenute nell'art. 14 della legge 3 agosto 1998 n. 269.

svolgimento delle operazioni, di essere sottoposto all'atto coercitivo, tanto da avere diritto ad una serie di adempimenti in chiara funzione garantistica. Quanto appena rilevato si estende altresì alle "nuove" forme di perquisizione introdotte dalla più volte citata L. n.48 del 2008 e inserite al comma 1 bis dell'art. 247 del c.p.p. . Pertanto, anche nel caso in cui tali perquisizioni abbiano per oggetto sistemi informatici o telematici, esse rimangono indirizzate alle medesime finalità di ricerca di cose pertinenti al reato e risultano sempre presidiate dagli ordinari diritti difensivi (a differenza appunto delle perquisizioni *online*).

2.3.f) Le perquisizioni *online* e le intercettazioni telematiche: differenze.

Alla stregua di quanto riportato nel precedente paragrafo, si potrebbe "azzardare" un facile accostamento delle perquisizioni online alle intercettazioni, specie di comunicazioni informatiche o telematiche (art. 266 bis c.p.p.): anche le intercettazioni, d'altra parte, durante il loro svolgimento, devono restare ignote al soggetto attinto (di regola, ma non necessariamente, l'indagato). L'iniziale, suggestiva similitudine lascia peraltro il campo a insormontabili differenze. Come noto, il "*common core"* delle intercettazioni è dato dalla "*captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere altri e con modalità oggettivante idonee allo scopo"*[145]*:* definizione che si deve ritenere applicabile anche alle intercettazioni di comunicazioni informatiche o telematiche intercorrenti tra utenti del web.
Sia ben chiaro: ove le perquisizioni *online* fossero preordinate a (o comunque consentissero nel concreto di) captare delle conversazioni tra utenti, il tutto si risolverebbe in una intercettazione ai sensi dell'art. 266 bis c.p.p., obbligando al rispetto delle forme ivi previste e comportando, in caso di inosservanza l'inutilizzabilità degli esiti (art. 271, comma 1, c.p.p.). Ma non è questo il fenomeno su cui si vuol portare l'attenzione (se non altro perché esso, risolvendosi in una intercettazione illegittima, troverebbe già una compiuta disciplina, anche sanzionatoria): le perquisizioni *online* sono concepite per ottenere un elevato numero di informazioni utili senza alcuna necessità di percepire comunicazioni in atto tra utenti, bensì semplicemente attraverso la sistematica o periodica raccolta di dati presso il sistema informatico utilizzato dall'indagato (*online search*) od attraverso la registrazione dei suoi movimenti sul web (*online surveillance*). Le risultanze cui esse danno luogo, quindi, dovrebbero essere considerate alla stregua degli innumerevoli dati che possono desumersi dai cc.dd. tabulati telefonici rispetto ai quali, come noto, la giurisprudenza di legittimità e le norme sui *"data retention"* (vedi *supra* para. 1.4.e)) hanno ricostruito una disciplina che, escludendo qualsivoglia intervento da parte del Gip, è esclusivamente imperniata sulla figura del P.M.[146]

[145] Cass. Sez. VI del 9.02.2005, n.12189, Rosi.

[146] Peraltro - come si vedrà infra al para. 4.2 - tra i molteplici dati che i gestori e gli operatori comunque denominati sono tenuti a conservare per finalità di Giustizia e Sicurezza, vengono espressamente

A questo proposito, premesso che, sotto il profilo tecnico, “muoversi" nella rete comporta necessariamente l'invio ed anzi lo scambio di dati tra più sistemi informatici o telematici (il proprio e, quantomeno, quello del provider del servizio), giovi la seguente precisazione: captare tali dati i integra senza dubbio, in astratto, il reato di cui all'art. 617 quater, co.1 c.p. - che punisce, tra l'altro, l'apprensione di comunicazioni *“intercorrenti tra più sistemi”*- ma non integra ancora l’intercettazione di comunicazioni processualmente rilevante, la quale richiede, rispetto alla norma sostanziale, un *quid pluris*: che le comunicazioni cioè intercorrano non tra meri sistemi informatici, bensì tra utenti, vale a dire tra persone fisiche che agiscono con l'intenzione di comunicare l'una con l'altra a mezzo della rete e che a tal fine si avvalgono di detti strumenti informatici. Ecco che allora risulta chiaro, per sottrazione, il possibile oggetto ed il concreto carattere discretivo delle perquisizioni *online*: per non ricadere infatti sotto la disciplina “tipica” delle intercettazioni (informatiche e/o telematiche), esse devono presentare, quale risultato ultimo, l'apprensione di dati aventi obiettivamente (per ricorrere ad un’espressione di recente utilizzazione da parte della giurisprudenza di legittimità[147]) carattere *"non comunicativo".*

2.3.g) Perquisizioni *online* come pedinamenti (*online*): differenze.

Potrebbe allora, da ultimo, venir naturale accostare le perquisizioni *online* al pedinamento, atto questo pure (o forse appunto proprio perchè) atipico di indagine, e ciò magari mediante il suggestivo accostamento dello spazio fisico in cui si svolge il pedinamento con lo sterminato spazio virtuale (il web) in cui potrebbe avvenire la perquisizione online. Ma anche tale accostamento è fallace ed anzi consente di porre un punto fermo da cui muovere per ogni successiva riflessione.

Ed in effetti, se l'accostamento avvenisse per applicare alla perquisizione online la disciplina del pedinamento, sarebbe chiaro l'errore. La giurisprudenza, infatti, ritiene che il pedinamento sia atto di indagine atipico di polizia giudiziaria e che non sia intrusivo della sfera privata, perché non limiterebbe, diversamente dai mezzi di ricerca della prova, la libertà morale del controllato[148].

All’opposto, le perquisizioni online, nella loro possibile veste di *“forme di pedinamento virtuale”*, consentirebbero agli organi dell’investigazione di raccogliere una mole impressionante di “dati personali” del soggetto interessato (ma anche di soggetti totalmente estranei alle indagini) e quindi di incidere in modo significativo e potenzialmente drammatico sul bene giuridico costituito dalla c.d. “riservatezza dei dati personali”[149] per di più, come si faceva notare, riferibili a soggetti possibilmente avulsi dall’indagine. Prova ne è che un’arbitraria attività di perquisizione *online* messa

---

escluse le informazioni relative ai contenuti (ed agli stessi indirizzi) dei siti e delle pagine web visitate dall’utente.

[147] Cass. Sez. Un. 28.03.2006 n. 26796, Prisco;

[148] Cass. Sez. II 30.10.2008 n.44912 *cit.*;

[149] Secondo la definizione data dall'art. 4, comma 1, lett, b) d.lg. 30 giugno 2003, n. 196, c.d. codice della privacy;

in atto da chi (non appartenente agli organi giudiziari procedenti) possegga gli opportuni strumenti conoscitivi e le relative capacità tecniche, porterebbe quasi sicuramente alla violazione di una norma penale incriminatrice (art. 615 *ter* se non art. 617 *quater* c.p.)[150]. Laddove una mera attività di pedinamento, ove non sconfini in un'azione persecutoria *(stalking)* o altro, non si porrebbe, in questi termini, in contrasto con l'ordinamento penale.

2.3.h) segue: Le perquisizioni online. Riflessioni conclusive.

Benché "atipiche" - al pari di ogni altro strumento di ricerca della prova, anche le perquisizioni *online* dovrebbero rendersi rispettose dei diritti e delle libertà dei singoli – con particolare riguardo alle posizioni soggettive direttamente contemplate e tutelate dalla Costituzione – non potendosi ovviamente compiere in assoluta libertà per il solo fatto di non essere state positivizzate in alcuno schema legale.

Bisogna pertanto stabilire quali interessi, diritti e libertà siano chiamati in causa nel momento in cui le perquisizioni *online* vengano poste in essere e, conseguentemente, ricercare proprio nel dettato costituzionale le garanzie e le prescrizioni necessarie affinché le stesse possano essere validamente esperite. Ora, questa indefettibile esigenza (addirittura di rango costituzionale), ci pone di fronte alla banale constatazione che, essendo le perquisizioni *online* ontologicamente diverse dalle omonime perquisizioni previste e disciplinate dal codice di procedura penale, e non essendo preordinate in ultima analisi a ricercare unicamente (come si evidenziava nel para.2.3.e)) il corpo del reato (o cose comunque pertinenti al reato), le stesse, nel momento in cui vengono disposte, si caratterizzano per la completa inconsapevolezza e addirittura imprevedibilità dei dati, delle notizie e delle informazioni che in concreto andranno a collazionare (un po' come il pescatore che getta le reti!). E non si tratta unicamente di salvaguardare la *privacy*[151] di tutti i soggetti comunque coinvolti nell'attività di ricerca probatoria (soggetti che come detto *supra* potrebbero essere del tutto estranei ai fatti per i quali si procede), ma - circostanza questa assai più rilevante - potrebbero essere raccolti dati ed informazioni a "carattere comunicativo" implicando per ciò solo una virtuale e non prevista captazione di comunicazione fra soggetti che si sostanzierebbe, in definitiva, in un'indebita[152] attività di intercettazione[153].

In altri termini, proprio per l'intrinseca natura di iniziative ad ampio spettro, le cc.dd. perquisizioni *online* spesso offrono contezza di quanto raccolto soltanto *a posteriori*, in un momento successivo, e questa loro peculiare caratteristica potrebbe pertanto condurre alla vanificazione di lunghe e complesse attività investigative qualora le

[150] Cfr. *supra*, rispettivamente ai para. 2.2.c) e 2.2.f).

[151] Per la cui tutela la Carta costituzionale non prevede peraltro alcuna specifica riserva di legge e/o di giurisdizione.

[152] Qualora ad esempio fosse stata disposta unicamente dal PM con proprio decreto motivsto.

[153] Ciò, in realtà, potrebbe verificarsi, quasi esclusivamente; nell'ambito della modalità esecutiva della perquisizione *online* nota come *online surveillance*

attività svolte non fossero corredate dalle garanzie e dalle tutele all'uopo imposte dall'ordinamento giuridico.
Il medesimo ragionamento porterebbe peraltro ad ulteriori complicazioni interpretative ove si riflettesse sull'intrinseca natura dello spazio virtuale ricoperto dall'ambito di operatività di un "personal computer"[154].
Ora, non sarebbe peregrino scorgere nel personal computer, così come peraltro suggeriscono moderne teorie sociologiche[155], una propaggine del proprio domicilio, ovvero un prolungamento del proprio spazio vitale, atteso che sovente tra le cartelle e i *file* del proprio PC (tablet, smartphone etc.) vengono custoditi o rappresentati in forma digitale situazioni, stati e contingenze afferenti alla sfera più intima della propria personalità e degli interessi economici, affettivi e familiari dell'individuo. Di conseguenza, non può non tenersi conto del duplice ordine di riserva (di legge e di giurisdizione) prescritta dall'art. 14 Cost. di talché, una qualsiasi "intrusione" investiga in questo vero e proprio "domicilio virtuale", lungi dal potersi espletare sulla base di atti atipici, dovrebbe invece trovare puntuale disciplina in una descrizione analitica norma di legge[156].
In conclusione, al fine di evitare che importanti elementi probatori possano andare espunti dal procedimento poiché acquisiti in violazione delle garanzie apprestate dall'ordinamento, sarebbe opportuno, a sommesso parere di chi scrive – nonostante le diversità concettuali, operative e strutturali evidenziate al para. 2.3.f) – che le perquisizioni *online* venissero "maneggiate" con la stessa circospezione, per gli stessi casi e alla luce delle medesime prescrizioni normative contenute negli artt. 266 bis e ss. c.p.p..

2.3.i) La localizzazione satellitare

Come si evidenziava al para 2.3.g), non sono mancati in dottrina tentativi tesi a ricondurre le perquisizioni *online* al pedinamento quale, appunto, atto atipico di indagine. Tuttavia, come ampiamente dimostrato, anche tale accostamento è dstinato a dimostrarsi fallace ed anzi consente di porre un punto fermo da cui muovere per ogni successiva riflessione.
In effetti, se l'accostamento avvenisse per applicare alla perquisizione *online* la disciplina del pedinamento (anzi, come si vedrà meglio *infra,* l'assenza di qualsivoglia disciplina positiva), sarebbe chiaro l'errore. La giurisprudenza, infatti, ritiene che il pedinamento sia atto di indagine atipico di polizia giudiziaria e che non sia intrusivo

[154] Che nei paesi anglosassoni viene indicato anche con l'espressione *"home computer*".

[155] L. Paccagnella, *La comunicazione al computer. Sociologia delle reti telematiche*, Il Mulino Bologna 1^ed.2000.

[156] Il legislatore aveva già considerato il sistema informatico un' espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli art. 614 e 615 C.P. (cosi la relazione al Disegno di Legge n. 2773 presentato al Senato il 26 marzo 1993 e trasferito alla Camera 1'11 giugno 1993).

della sfera privata, perché non limiterebbe, diversamente dai mezzi di ricerca della prova, la libertà morale del controllato[157].

All'opposto, le perquisizioni *online*, nella loro possibile veste di "forme di pedinamento virtuale", consentirebbero agli organi dell'investigazione di raccogliere una mole impressionante di "dati personali" del soggetto interessato (ma anche di soggetti totalmente estranei alle indagini) e quindi di incidere in modo significativo e potenzialmente drammatico sul bene giuridico costituito dalla c.d. "riservatezza dei dati personali"[158].

Più o meno negli stessi termini si è posta una questione affine alla precedente.

Merita di essere ricordato, difatti, come tra i principali sistemi telematici utilizzati in ambito investigativo un ruolo importante è sicuramente svolto dal c.d. *tracker GPS* (acronimo di *Global Positionig System*): un dispositivo cioè in grado di monitorare gli spostamenti dell'oggetto — di regola un veicolo, ma non solo — su cui viene installato o della persona che lo porta con sé[159].

Volendoci attenere al massimo della sintesi e della schematizzazione - seguendo il principio che, dalla prima all'ultima pagina, ha ispirato la realizzazione del presente lavoro - possiamo quindi semplicemente dire che il tracker GPS consente di localizzare un oggetto (ovvero un soggetto) e di seguirne i movimenti con elevata precisione sotto il profilo spazio temporale.

Passando direttamente ai problemi di ordine giuridico-sistematico, è d'uopo rilevare che il monitoraggio tramite *tracker* GPS integra (al pari, come si è visto, delle perquisizioni *online*) gli estremi di una mera modalità investigativa non espressamente disciplinata dal codice (atipica, per l'appunto). Ciò pone, conseguentemente, il problema di individuarne innanzitutto l'esatta configurazione giuridica, cominciando con il domandarsi se - nonostante il silenzio normativo - essa sia comunque riconducibile, in via interpretativa, ad un'attività investigativa nominata. In effetti, non mancano opinioni orientate in tal senso.

---

[157] Cass. Sez. II 30.10.2008 n.44912 *cit.*;

[158] Secondo la definizione data dall'art. 4, comma 1, lett, b) d.lg. 30 giugno 2003, n. 196, c.d. codice della privacy;

[159] Conviene, anzitutto, descrivere brevemente le caratteristiche tecniche di questo strumento, di così piccole dimensioni da poter essere contenuto nel palmo di una mano.
Esso si compone di due "sottosistemi" diversi.
Il primo è in grado di calcolare la posizione del dispositivo GPS e l'ora esatta della rilevazione. Un simile calcolo è possibile grazie all'utilizzo della tecnologia satellitare. Infatti, nella esosfera, cioè nello strato più esterno dell'atmosfera, sono collocati dei satelliti che emettono costantemente un segnale radio, il quale trasmette informazioni che riguardano l'ora di emissione, il codice identificativo e la posizione del satellite. Il "sottosistema" è in grado di ricevere segnali provenienti da satelliti diversi, che di regola non sono meno di quattro. E poiché esiste un solo luogo sulla terra che presenti una determinata distanza rispetto a ciascuno dei satelliti (almeno quattro) da cui è giunto il segnale, tramite un algoritmo è possibile individuare latitudine, longitudine ed altitudine del tracker GPS e, quindi, localizzarlo con precisione.
Mentre il primo "sottosistema" può soltanto ricevere i segnali ed eseguire l'algoritmo, un secondo "sottosistema" permette di trasmettere - mediante trasmissione di sms su rete GSM ovvero mediante la rete gprs, ovvero ancora (ma di rado per scopi investigativi e, quindi, per scopi essenzialmente militari) mediante telefonia satellitare - i dati relativi alla localizzazione e all'ora esatta della rilevazione ad un terminale (di regola un computer od un tablet) in possesso degli investigatori, il quale, per mezzo di un apposito software, elabora una mappa cartografica elettronica, che normalmente viene poi assicurata su un supporto informatico (DVD, CD-Rom, pendrive).

Alcuni vi vedono infatti, alla stregua di una concezione fortemente estensiva, una particolare varietà di intercettazione, sul presupposto che l'impiego della tecnica GPS determinerebbe una incisiva lesione della privacy del soggetto monitorato del tutto analoga, per ampiezza e lesività, a quella provocata da tale strumento investigativo. Sicché la localizzazione satellitare dovrebbe sottostare alla disciplina prevista dagli artt. 266-271 c.p.p.[160]

Peraltro, nonostante il codice non fornisca una definizione generale di intercettazione, sulla base dei limiti di ammissibilità fissati dall'art. 266 c.p.p. e della disciplina dell'intercettazione di comunicazioni informatiche o telematiche prevista dall'art. 266-bis c.p.p., si ritiene, come ampiamente illustrato *supra*, che tale mezzo di ricerca della prova implichi la captazione clandestina da parte di un soggetto terzo del contenuto di una comunicazione riservata tra due o più persone. Ora, se è vero che la localizzazione satellitare comporta certamente la captazione clandestina dei dati relativi all'ubicazione dell'oggetto (soggetto) su cui è installato il tracker GPS, è anche vero che con un simile monitoraggio non viene appresa alcuna comunicazione tra persone, dato che ci si limita a rilevare la mera posizione nello spazio dell'oggetto su cui è collocato il dispositivo GPS e, conseguentemente, del soggetto monitorato. E ciò dovrebbe essere sufficiente ad escludere che la localizzazione satellitare possa rientrare nel *genus* delle intercettazioni e che se ne possa applicare la relativa disciplina[161].

Neppure, come anche si è ritenuto, i dati di localizzazione satellitare potrebbero essere invece qualificati come *« dati relativi al traffico»* ai sensi del d. Ivo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, c.d. Codice della privacy) ed essere assimilati ai dati *"esteriori"* del traffico telefonico (cfr.. *supra* para. 1.4.e) e, soprattutto, i para. 4.2.a) e ss. *infra*), che, ai sensi dell'art. 132, comma 3 di quel "codice", possono essere acquisiti nell'ambito di un'indagine soltanto in forza di un decreto motivato del pubblico ministero. Anche in questo caso, infatti, è la mancanza di una "comunicazione" tra persone nella tecnica GPS ad apparire risolutiva: come ha chiarito il Garante della Privacy nel rispondere ad un quesito del Dipartimento di Pubblica Sicurezza proprio relativo alle modalità di acquisizione dei dati di localizzazione nell'ambito delle attività di polizia giudiziaria, quando tali dati prescindono da una comunicazione tra persone, essi non possono essere qualificati come dati di traffico soggetti alla disciplina cui all'art. 132 codice privacy[162].

---

[160] L.G. Velani. *Nuove tecnologie e prova penale: il sistema di individuazione satellitare g.p.s.*, in Giur. it., 2003, p. 2375; nonché D. Iacobacci, *Sulla necessità di riformare la disciplina delle intercettazioni prendendo le mosse dalle esitazioni applicative già note*, in Giust. pen., Ill, 2011, c. 365 ss., che, pur *«nella consapevolezza della forzatura esegetica»,* propone un'interpretazione estensiva della disciplina autorizzatoria delle intercettazioni telefoniche al fine di rafforzare le garanzie anche in riferimento alla localizzazione satellitare.

[161] In tal senso, *ex plurimis*, v. Cass, pen., Sez. I, 7 gennaio 2010, n. 9416; Sez. V, 15 dicembre 2009, n. 9667; Sez. VI, 11 dicembre 2007, n. 15369; in dottrina, Stramaglia, *Il pedinamento satellitare: ricerca ed uso di una prova "atipica",* in Dir. pen. proc, 2011, p. 214.

[162] Cfr.. Provv. 19 dicembre 2008 Garante per la protezione dei dati personali; Relazione 2010. Evoluzione tecnologica e protezione dei dati, Roma, 2011, p. 95; Id., *Parere al Ministero dell'Interno, 25 gennaio 2010*, in F. Caiani, *"I nuovi mezzi di ricerca della prova: videoriprese investigative, agente segreto attrezzato per il suono, pedinamento elettronico ed appostamenti informatici, installazione*

Ed ancora, la localizzazione satellitare non può neppure essere ricondotta, per ragioni che paiono di immediata percezione, all'ispezione, agli accertamenti urgenti o ai comuni rilievi (segnaletici, descrittivi o fotografici).

In realtà, il monitoraggio satellitare rappresenta - sia consentito il gioco di parole - una tipica attività "atipica" di indagine il cui corrispettivo per cosi dire *"analogico"* (cioè non digitale) è agevolmente individuabile nel c.d. pedinamento. Non sfugge infatti come la localizzazione satellitare possa rappresentarne una specifica modalità di svolgimento. Invero, poiché il pedinamento si identifica nell'attività di monitoraggio degli spostamenti di un soggetto, la localizzazione satellitare sembra a tutti gli effetti configurarsi come una *species* tecnologica di tale *genus*. Non a torto, quindi, si può parlare di "pedinamento elettronico". Del resto, un'assimilazione di questo tipo si rinviene anche in alcune prese di posizione del legislatore, per la verità poco conosciute, ove il monitoraggio GPS viene esplicitamente considerato come un'osservazione *«dinamica (c.d. pedinamento) anche a mezzo di strumenti elettronici»*[163] (d. m. 1 dicembre 2010 n. 269) ovvero come l'insieme dei *«mezzi tecnici, necessari per l'effettuazione [...] del pedinamento»* (L. 7 aprile 2011 n. 60)[164].

La dottrina pressoché unanime critica invece in maniera risoluta quest'impostazione, rimarcando come la tecnica GPS presenti rispetto al pedinamento una maggiore invasività, dato che essa consente di effettuare un monitoraggio estremamente preciso continuo e penetrante, anche in luoghi che non sarebbero altrimenti visibili e in rapporto ai quali, dunque, il pedinamento non sarebbe praticabile[165].

Alla stregua dell'art.189 c.p.p., si discute inoltre circa la reale *"idoneità asseverativa"* dei fatti attribuibile al monitoraggio tramite GPS (quale strumento di ricerca della prova non disciplinato da alcuna norma di legge). Il predetto requisito infatti potrebbe, in concreto, venire compromesso nella sua funzionalità, dall'impiego ad opera della criminalità di sistemi in grado di pregiudicarne il corretto funzionamento[166].

---

di captatori infc informatici, in AA. VV. Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici, vol. II, Forlì, 2011, p. 443 ss.

[163] Cfr. art. 5, comma 1, lett. a.VI) d. m. 1 dicembre 2010 n. 269. V. anche Disposizioni operative per l'attuazione del D.M. 1 dicembre 2010, n. 269, in materia di capacità tecnica e qualità dei servizi degli istituti di vigilanza ed investigazione privata, a cura del Dipartimento di Pubblica Sicurezza - Ufficio per l'Amministrazione Generale - Ufficio per Affari della Polizia amministrativa e sociale, Circolare 557/PAS/U/004935/ 10089.D(l)Reg, p. 13, la quale fa testuale riferimento ai «pedinamenti (anche a mezzo di rilevazioni elettroniche con apparecchiature GPS) ».

[164] Si tratta della legge di ratifica ed esecuzione dell'Accordo tra il Governo della Repubblica italiana e il Governo della Repubblica di Slovenia sulla cooperazione transfrontaliera di polizia.

[165] In questo senso, ad es. Manchia, *Localizzazione tramite gps, quali garanzie?* In RG Sarda, 2006, p.432; Laronga, *Il pedinamento satellitare: un atto atipico lesivo di diritti inviolabili?* QG, 2002, 1157; Scaglione, *Attività atipica di polizia giudiziaria e controllo satellitare*, in Foro Italiano 2002, p.635; Peretoli, *Controllo satellitare con GPS: pedinamento o intercettazione?* in Dir. pen. e processo, 2003, p. 94;

[166] Potrebbe trattarsi di un c.d. *jammer* (usato magari "a singhiozzo" dai criminali sotto osservazione)*:* un dispositivo cioè in grado di "schermare" il segnale satellitare e di impedire, quindi, al *tracker* GPS di individuare le proprie coordinate. Ma potrebbe venire adoperato anche un dispositivo, di recente realizzazione, capace di svolgere un'attività di "disorientamento" (c.d. GNSS *spoofing*) del tracker GPS, inducendolo ad elaborare dati di ubicazione dalle coordinate errate e perciò inattendibili, con conseguenze irreversibili sul piano della sua idoneità accertativa.

Infine, va qui fatto soltanto cenno (sì estesa è l'ampiezza delle sue implicazioni) ad una questione di grande importanza teorico-pratica posta al centro di un vivace dibattito dottrinale.

Si tratta cioè della conformità della tecnica del controllo satellitare alle norme della C.e.d.u. (ed in particolare all'art.8) alla stregua della disciplina – o meglio della totale assenza di disciplina (anche solo di esclusiva derivazione giurisprudenziale) – del pedinamento tramite GPS; e questo in considerazione della totale assenze di, sia pur minimali, garanzie in ordine ad un'attività che potrebbe rivelarsi - qualora protratta per lungo tempo ovvero disposta relativamente a reati puramente bagatellari - oltremodo invasiva della sfera di riservatezza ed intimità del singolo.

Sul punto, stigmatizzando recisamente la lacuna normativa che caratterizza le legislazioni dei Paesi aderenti alla Carta Europea dei Diritti dell'Uomo, la Corte di Strasburgo ha addirittura avuto più volte modo di affermare che *"(omissis)…i requisiti previsti dalle legislazioni dei singoli Stati in materia di intercettazioni….potrebbero eventualmente costituire degli orientativi punti di riferimento anche in tema di localizzazione satellitare…"*[167].

[167] Cfr. Corte EDU, Uzun vs. Germania, 2 settembre 2010. Per un'analisi approfondita cfr. Signorato, La localizzazione satellitare nel sistema degli atti investigativi, in Rivista italiana di diritto e procedura penale, II, 2012, pp. 580 ss. ;

Capitolo III: le intercettazioni del voip

***

"The time to repair the roof is when the sun is shining"
(Kennedy, John F.)

3.1 Voip e tecnologie di intercettazione: tra vecchio e nuovo.

3.1.a) Premessa

Letteralmente l'acronimo VOIP sta per "*Voice Over Internet Protocol*". Si tratta di una tecnologia relativamente recente, ma che si è ormai fortemente consolidata. La principale funzionalità del Voip consiste nella possibilità di effettuare una vera e propria conversazione telefonica sfruttando una preesistente connessione di rete (può trattarsi o di una connessione internet ovvero di un'altra rete all'uopo dedicata che utilizza il protocollo IP) anziché passare attraverso la rete telefonica tradizionale (PSTN- *Public switched telephone network*).
La grande particolarità del voip rispetto alle comunicazioni telefoniche tradizionali si rinviene nel fatto che, nell'ambito del suo funzionamento, vengono del tutto eliminate le centrali di commutazione. Il sistema Voip infatti, attraverso appositi softwares (chiamati *gateways*), provvede ad instradare sulla rete pacchetti di dati contenenti le "informazioni vocali" (analogiche) codificate e compresse in forma digitale (*bits*), solo nel momento in cui è necessario cioè quando uno degli utenti collegati sta parlando.
Ora, come si accennava in precedenza, le conversazioni mediante voip non debbono necessariamente viaggiare su internet, ma possono utilizzare quale via di trasmissione una qualsiasi rete privata basata sul protocollo IP, ad esempio una rete LAN (*local area network*) all'interno di un edificio o blocco di edifici.
Ma non solo, le conversazioni tramite voip possono anche sfruttare la rete telefonica tradizionale (fissa e mobile), dando luogo ad una pluralità di combinazioni e modalità di interconnessione:

- Da PC a PC;
- Da PC verso un telefono (fisso/cellulare/satellitare);
- Da telefono voip a telefono voip/telefono tradizionale (fisso, mobile, satellitare);

In estrema sintesi[168], i tre principali vantaggi del voip rispetto alla telefonia tradizionale, possono così riassumersi:

- Minori costi per le chiamate;
- Costi infrastrutturali assolutamente trascurabili (in pratica è sufficiente una qualsiasi connessione IP);
- Possibilità di implementare nuove opzioni e funzionalità senza alcun bisogno di sostituzione hardware.

[168] Come bene viene evidenziato sulla enciclopedia online Wikipedia alla voce "*Voip".*

In un primo momento il voip è stato utilizzato in forma sostanzialmente elitaria da grandi multinazionali e/o in ambito imprenditoriale. Attualmente però la diffusa disponibilità del web a banda larga e la particolare facilità di utilizzo del più noto modello di fruizione di telefonia via internet[169], hanno decretato la diffusione capillare del Voip anche in ambito professionale e soprattutto tra privati.
Ma non soltanto, va altresì debitamente ricordato come la legge finanziaria per l'anno 2008 imponga (a partire dal 1° gennaio di quell'anno) a tutti gli enti pubblici - allo scopo di razionalizzare le risorse e contestualmente diminuire i costi della P.A. - di convertire la propria utenza telefonica analogica al voip.
Peraltro, al fine di assicurare la piena attuazione di detta disposizione, il legislatore ha, da un lato, affidato al CNIPA (Centro nazionale per l'informatica nella PA) il compito di verificarne la piena attuazione e, dall'altro, ridotto drasticamente, per gli anni successivi all'entrata in vigore del provvedimento, gli stanziamenti relativi alle spese di telefonia delle Pubbliche Amministrazioni[170].

3.1.b) Intercettazioni di apparati voip: intercettazioni telefoniche o telematiche?

Le ragioni storico-sistematiche alla base dell'introduzione nel nostro ordinamento - a metà degli anni novanta, in aggiunta alle ordinarie captazione di comunicazioni telefoniche - delle intercettazioni di comunicazioni informatiche e telematiche sono da ricercarsi, come detto *supra* (para. 1.3.a), nella presa di coscienza da parte del legislatore italiano dell'interesse sempre crescente che le organizzazioni criminali mostrano verso tutti i nuovi portati della tecnica che consentono comunicazioni rapide, efficienti ed altamente sicure.
D'altra parte, la disciplina delle nuove tipologie di intercettazioni venne per molti aspetti modellata su quella delle intercettazioni ordinarie[171], prevedendo però al contempo una serie di aspetti normativi ed operativi del tutto autonomi e pertanto di specifico interesse ermeneutico[172].
Fu rilevato ad esempio come già l'art. 266 c.p.p. non limitasse la sua previsione all'intercettazione di conversazioni o comunicazioni telefoniche, ma contenesse già un, sia pur generico, riferimento ad *"altre forme di telecomunicazioni"* (art. 266 co.1 C.p.p.), si da consentirne un adattamento automatico ogniqualvolta ulteriori acquisizioni della scienza lo avessero richiesto. Ed infatti, ancor prima della emanazione della legge 547//1993 si faceva rientrare il concetto di intercettazione telematica, nel novero della disciplina delle intercettazioni di comunicazioni ex art. 266 co. 1 lett. f) (ove appunto si parla di "altre forme di telecomunicazioni"), ma è

[169] Skype, su cui ci soffermerà a lungo *infra.*
[170] Per comprendere la portata e l'importanza di questo provvedimento, si pensi soltanto alla mole enorme di comunicazioni telefoniche che annualmente intercorrono tra la Farnesina e le rappresentanze diplomatiche e consolari sparse per il mondo
[171] Quelle cioè contemplate dagli artt. 266 e ss. c.p.p. cfr. *supra*
[172] Per la disamina dei quali si rinvia al para. 1.3.c), *supra.*

altrettanto vero che detta sussunzione, oltre ad esporre ai "pericoli"[173] connessi all'estensione analogica delle norme in tema di intercettazione, dava luogo ad una equiparazione che appare immediatamente priva di fondamento qualora si proceda ad una analisi delle informazioni trasmesse via telefono, contrapponendole a quelle trasmesse via computer.

Le intercettazioni telefoniche consentono infatti di inserirsi in una trasmissione "fonica" passante per una linea dedicata o commutata: sono, quindi, in grado di accertare che sia in corso una comunicazione, che ci sia uno scambio di impulsi, tra modem. Non sono in grado però di decifrarne il contenuto. Ed è proprio per l'attività di decifrazione delle informazioni trasferite via modem che è stata predisposta l'intercettazione telematica: i suoni o gli impulsi trasmessi via computer vengono infatti intercettati e decifrati in informazioni interpretabili da un altro computer (a disposizione degli inquirenti) che le renderà comprensibili all'uomo.

Sennonché, per ciò che riguarda direttamente la comunicazione tramite voip (nei termini in cui è stata descritta), a fronte di una interpretazione tutta incentrata sulla natura della comunicazione (che attenendo alla voce umana dovrebbe considerarsi pienamente sussumibile alla previsione cui all'art. 266 c.p.p.), si contrappone la necessità sia tecnica che teorica di considerare la relativa intercettazione come "telematica" ex art. 266-bis c.p.p.

Ed infatti, a conferma della possibilità di ricomprendere l'intercettazione voip tra quelle telematiche, militano almeno quattro argomenti, e precisamente:

1) Il riferimento dell'art. 266 c.p.p. ad "altre forme di telecomunicazione" deve intendersi pacificamente a quelle già esistenti all'epoca della sua introduzione: si pensi al mezzo del citofono o dell'interfono (per le conversazioni da intercettare in carcere); *(c.d.dato storico)*;
2) La legge 547/93 conferma l'impostazione di cui al precedente punto, dal momento che - introducendo espressamente una nuova norma sul punto - conferma che "le altre forme di telecomunicazione" non sono quelle informatiche; *(c.d. dato sistematico);*
3) Quanto alla conformità di tale interpretazione ai dettami dell'art. 3 Cost., va rilevato che i differenti limiti edittali dei reati per i quali è possibile disporre un'intercettazione (non contemplati per le intercettazioni telematiche ed invece elevati e tassativi rispetto alle intercettazioni telefoniche) non sono certo una novità. Infatti la richiamata lett. f) dell'art. 266 c.p.p. stabilisce chiaramente che quello che rileva è il "mezzo" utilizzato (indipendentemente dal tipo di reato da sottoporre ad intercettazione). Allo stesso modo il mezzo del personal computer necessita, proprio per sua diffusività (ed invasività) in termini di commissione di reati da parte della criminalità, una uguale risposta in termini di mezzi di accertamento dei fatti da mettere a disposizione degli investigatori *(ulteriore dato sistematico)*.

[173] In questo senso Sarzana op. cit.

3.1.c) segue. Sistemi telefonici e sistemi telematici. Una distinzione "sfumata".

Il quarto ed ultimo dato è quello che potremmo definire: *giurisprudenziale*.

Nell'ambito di un'importante sentenza emessa a Sezioni Unite, la Corte di Cassazione[174] proclama infatti senza tentennamenti la riconducibilità al concetto di *sistema telematico* dell'intero sistema telefonico mobile, statuendo: *<< La moderna telefonia mobile si svolge col sistema cellulare (trasmissione tramite rete di terra) o satellitare (il segnale giunge a destinazione via satellite), ma anche quella fissa si è adeguata alle nuove tecnologie. In particolare, fu introdotto il sistema cellulare di tipo analogico non ancora adatto alla trasmissione di dati (apparecchi AMPS, TACS, ETAX) e che utilizzava la modulazione di frequenza…(omissis…). In concreto* – continua la Corte - *le linee telefoniche, secondo la moderna tecnologia, attuano la trasmissione delle comunicazioni con la conversione (codificazione) di segnali fonici in forma di "flusso" continuo di cifre, e detti segnali, trasportati all'altro estremo, vengono ricostruiti all'origine (decodificazione)…(omissis) . Trattasi, dunque, di flussi relativi ad un sistema tecnico che s'innesta nella disciplina delle intercettazioni di comunicazioni informatiche o telematiche, captate a sorpresa nel corso del loro svolgimento, che hanno per oggetto anche la posta elettronica (e-mail) da computer a computer collegati alla rete internet in forma ibrida per mezzo di SMS da computer (collegato alla detta rete) ad apparecchi cellulari GSM o vice-versa. Il flusso è il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici. Fra strumenti informatici, quindi, è possibile lo scambio di impulsi in cui si traducono le informazioni; scambio che è comunicazione al pari della conversazione telefonica, sicché la relativa captazione nel momento in cui si realizza costituisce intercettazione>>"*. *<<Omissis…il sistema telefonico mobile deve ormai essere considerato ai sensi dell'art. 266-bis…(omissis)…>>*.

Ma già in precedenza, la Suprema Corte, riferendosi al servizio (*idest* sistema) di telefonia fissa così si esprimeva[175]: *<<…un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate – per mezzo di un'attività di "codificazione" e "decodificazione" – dalla "registrazione" o memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "Dati" cioè di rappresentazioni elementari di un fatto, effettuate attraverso simboli (bit), in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni" costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente."*

Dalle due precedenti Massime si deduce agevolmente come l'intero sistema telefonico a disposizione degli utenti (fisso e mobile) - e indirettamente l'intero

[174] Cass. Sez Un., 23 febbraio 2000, n. 6 - D'Amuri, in Cass. Pen., 2000, 1419

[175] Cass. Sez. IV, 14 dicembre 1999,CED 214945.

sistema delle intercettazioni disposte dalla A.G. - dovrebbe oggi pacificamente identificarsi in un gigantesco e complesso sistema telematico (ex art 266 bis c.p.p).
Pertanto deve ritenersi definitivamente sfumata la differenza (potremo dire) *"ontologica"* tra comunicazione telefonica tradizionale e comunicazione telematica.
La ricostruzione giurisprudenziale pertanto non mancherà, presto o tardi, di riverberare i propri effetti anche sul dettato normativo e sulla (tuttora) esistente distinzione nominalistica e di disciplina tra intercettazioni telefoniche ed intercettazioni telematiche; circostanza peraltro che si renderà tanto più necessaria quanto più incisivamente la tecnologia voip riuscirà a rivoluzionare, con l'implementazione di sempre nuove ed inedite funzionalità, l'universale fenomenologia delle telecomunicazioni.
Va aggiunto però che non mancano opinioni di segno opposto orientate cioè a ridimensionare l'odierna obiettiva difficoltà di distinzione tra intercettazioni telematiche ed intercettazioni vocali *tout court* in virtù del predetto accentuato fenomeno di convergenza tecnologica (con conseguente digitalizzazione dei tradizionali servizi di telefonia). I fautori di questa concezione individuano nelle indicazioni del legislatore, infatti, la volontà di distinguere nettamente tra la conversazione orale tra due (o più) soggetti, a prescindere dal mezzo attraverso cui avviene, e il mero trasferimento di dati. Deve rimanere inalterata pertanto l'impostazione tradizionale in base alla quale per i reati informatici meno gravi, non può considerarsi esperibile l'intercettazione ex art. 266 c.p.p. Ed è' proprio alla luce di queste premesse che – si ritiene - sarebbe possibile risolvere la questione relativa al regime giuridico appropriato cui sottoporre le chiamate vocali effettuate tramite Voip.

3.1.d) La disciplina regolatrice del voip: l'approccio *(soft)* europeo.

Nel (recente/lontano? – sic!) mese di febbraio 2004, dopo una lunga fase di consultazione pubblica, vennero pubblicati: "l'Approccio comune della Commissione Europea sul voip"; ed il *"Common Statement for VOIP Regulatory Approaches"* ad opera dell'ERG (European Regulatory Group)[176].
Alla stregua dei principi di neutralità tecnologica[177] e sussidiarietà, ed in considerazione della portata potenzialmente rivoluzionaria dell'innovazione

[176] Si tratta del *forum* formale delle 25 Autorità nazionali di regolazione istituito dalla Direttiva quadro.

[177] Noto anche come "*net/network neutrality",* è il principio in ossequio al quale i fornitori di servizi internet sono tenuti a non operare alcuna discriminazioni fra differenti fonti di dati e di traffico web. Il problema della *network neutrality* evidenzia un profilo tecnico la cui soluzione è connessa all'individuazione del giusto equilibrio tra la parte di banda (e di rete) da dedicare a servizi che necessitano di una gestione a*d hoc* e la parte di banda che deve comunque continuare a garantire l'accesso a internet sulla base del principio del *best effort*. Tale equilibrio riveste particolare rilevanza sotto due aspetti: tutela del consumatore nella sua libertà di accedere ai contenuti su internet senza restrizioni; tutela degli operatori ad ottenere una remunerazione per i servizi offerti in rete. Alla base del principio di neutralità tecnologica risiede quindi la necessità di favorire il benessere dei consumatori, cioè la possibilità, da parte degli stessi, di aver accesso ai contenuti,

tecnologica che cominciava ad affacciarsi nel settore delle telecomunicazioni, i due provvedimenti concordavano nel ritenere - atteso lo stato ancora embrionale in cui si trovava, a quel tempo, il mercato del voip ed al fine di non pregiudicarne il futuro sviluppo - di non dover indicare particolari interventi regolatori rispetto a quelli già adottati con riguardo alla generale categoria delle comunicazioni elettroniche[178], limitandosi ad auspicare, per il momento, una sostanziale dimensione di *soft regulation*, rimandando ad un periodo successivo l'eventuale soluzione di problematiche intrinseche e peculiari alla neonata tecnologia.

Pertanto, dopo un breve periodo di "decantazione", l'autorità preposta al settore delle comunicazioni (AGCOM) è intervenuta a cadenza periodica sullo specifico settore del voip, attraverso delibere tese a suffragare i principi di carattere generale e ad impartire, all'occorrenza, sporadiche norme di dettaglio.

Merita di essere segnalato il distintivo *modus operandi* dell'Autorità delle Comunicazioni[179] la quale, tutte le volte in cui si è proposta di intervenire sulla particolare materia, ha preliminarmente cercato ed ottenuto l'intervento, in sede consultiva, dei principali operatori di settore e ciò sia al fine di accertare lo stato dell'arte del momento sia allo scopo di adottare regole di disciplina che fossero le più condivise possibili. Le norme in concreto adottate, peraltro, si pongono all'interno dell'alveo indicato dalle direttive europee e si mostrano sempre tendenzialmente rispettose del principio di *soft regulation* auspicato in seno alle Istituzioni dell'Unione Europea.

Così, con la delibera n° 11/06/CIR[180] l'AGCOM ha iniziato a fissare i primi paletti di riferimento, prevedendo, fra l'altro, il rilascio da parte del Ministero dello Sviluppo economico[181] di *un'autorizzazione generale* per la fornitura del servizio. Dalla titolarità della predetta autorizzazione discendono quindi per gli operatori una variegata serie di diritti e, quale corrispettivo, un certo numero di obblighi. I principali:

- garantire l'interoperabilità e l'interconnessione (tra loro) dei servizi offerti;
- concedere un accesso alle interfacce tecniche, ai protocolli e ad altre tecnologie indispensabili per l'interoperabilità dei servizi VoIP;
- utilizzare protocolli standard, ove praticabile (art 20 Codice delle comunicazioni elettroniche).

I precedenti punti peraltro sono stati ulteriormente sviluppati e convenientemente definiti dalla delibera n°128/2011 dell'AGCOM che, dettando *"disposizioni*

---

senza discriminazione tra le reti di trasmissione. Oggi l'art. 4 co. 3 lett. h) del Codice delle comunicazioni elettroniche (così come modificato dal D.leg.vo n° 70 del 28 maggio 2012) individua in detto principio "*uno degli obiettivi generali della disciplina di reti e servizi di comunicazione elettronica".*

178 Direttiva 2002/21; Direttiva 2002/20; Direttiva 2002/19; Direttiva 2002/22; Direttiva 2002/58, le quali complessivamente considerate, costituiscono il *c.d. New Regulatory Framework (NFR) for electronic communications.*

179 *Modus operandi* prescritto fra l'altro dall'art. 20 del Codice delle comunicazioni elettroniche.

180 *"Disposizioni regolamentari per la fornitura di servizi voip (voice over internet protocol) e integrazione del piano nazionale di numerazione".*

181 Al tempo, delle "Telecomunicazioni".

regolamentari in merito alla interconnessione IP e interoperabilità per la fornitura di servizi voip", ha altresì previsto protocolli specifici e puntuali modalità tecniche che i fornitori di servizi voip autorizzati sono tenuti ad implementare allo scopo di garantire ottemperanza agli obblighi di prestazione nei confronti della Autorità Giudiziaria.

3.1.e) Intercettabilità delle comunicazioni Voip e prestazioni obbligatorie[182].

Il tema della intercettabilità delle comunicazioni voip deve essere affrontato sulla base di una preliminare, essenziale, distinzione dei profili tecnologici.
Da un lato, infatti, si pongono i sistemi VoIP che si basano su protocolli proprietari e che - come nel caso di Skype (almeno fino a quando non venne acquisita da Microsoft nel maggio del 2011 cfr. nota al titolo *supra)* - si avvalgono di protezioni crittografiche robuste in virtù delle quali, stante la indisponibilità delle chiavi, non risulta possibile la decifratura del contenuto della telefonata (ancorché intercettabile ed intercettata a livello di traffico telematico) o, meglio, la rendono teoricamente ipotizzabile, ma con una tempistica assolutamente indefinita ed a fronte di costi (per l'utilizzo di centri di calcolo performanti) incompatibili rispetto a quelli della giustizia.
Dall'altro, vi sono invece i sistemi che si basano sui protocolli standard SIP o H.323, per i quali, quando si omettono le protezioni crittografiche (scelta compiuta di frequente per evitare un degrado delle prestazioni) non si pongono problemi di fruizione del contenuto intercettato, ed è pertanto pienamente applicabile, a livello

[182] Nel considerare le peculiari caratteristiche tecniche del principale *client* di telefonia voip (Skype) - nel presente paragrafo come nel prosieguo - spesso si ometterà deliberatamente di far riferimento alla nuova architettura di cui Skype è stata dotata quale conseguenza della sua acquisizione, nell'estate del 2011 (per 8,5 miliardi di dollari!), da parte di Microsoft Corp.
A voler dar credito ad alcuni *rumors,* il colosso informatico di Redmond avrebbe infatti mutato intenzionalmente la specifica struttura di funzionamento di Skype spostando, previa loro drastica riduzione, i supernodi (prima costituiti da tutti gli utenti) su *server* proprietari al fine di rendere tutto il traffico sottoponibile ad un unico sistema centralizzato e, quindi, potenzialmente monitorabile.
Ponendo fine, di fatto, alla peculiare e tradizionale architettura *peer to peer* di Skype ed utilizzando sistemi di decrittazione proprietari, Microsoft ha quindi definitivamente risolto la *querelle* che aveva visto duramente contrapposti i manager della piccola azienda di diritto estone (skype nasce infatti dall'intuizione di un ricercatore del piccolo stato baltico) - che riconducevano alla particolare architettura di funzionamento l'impossibilità di ottemperare alle prestazioni di giustizia ai fini di intercettazione – e le autorità giudiziarie e di polizia della maggior parte dei paesi europei nonché le stesse Istituzioni della U.E. che, nel 2009, avevano addirittura sollecitato l'apertura di un fascicolo in seno ad Eurojust.
Quali che siano le ragioni recondite di questa, per molti aspetti rivoluzionaria, rivisitazione strutturale dell'architettura di Skype (compiacenza/sudditanza nei confronti dei governi degli stati – USA in primo luogo – ovvero funzionalità più performanti e maggior qualità dei servizi offerti), l'iniziativa di Microsoft non elimina alla radice la possibilità che un nuovo e diverso operatore possa riproporre un servizio voip che ricalchi, più o meno negli stessi termini, il meccanismo di funzionamento tradizionale (*peer to peer*) di Skype.
Stante quanto sopra, si spiegano agevolmente le ragioni e le motivazioni che spingono nella direzione di voler continuare a considerare ancora pienamnte sussistenti ed attuali le peculiarità e le tematiche sussumibili alla trattazione delle problematiche di skype (per così dire) prima edizione!

procedurale, la normativa in materia di intercettazione dei flussi telematici (ex art. 266 bis c.p.p.).

In relazione alla prima tipologia di sistemi, ed in particolare al sistema Skype, è attualmente aperto un dibattito a livello internazionale, cui sono evidentemente interessati tanto gli organismi investigativi quanto le autorità giudiziarie ed amministrative competenti in materia di comunicazioni e focalizzato sia sulle tecniche e sulle procedure ipotizzabili - allo stato dell'arte - per la decifratura delle comunicazioni, sia sull'assoggettabilità del fornitore della soluzione VoIP agli obblighi che gravano sui gestori dei servizi di comunicazione pubblica, in termini di identificabilità degli utenti, conservazione traffico e fruizione dei contenuti della comunicazione[183] .

Quanto alla fruizione dei contenuti delle comunicazioni (*alias* concreta possibilità di effettuare intercettazioni), rispetto a Skype - almeno fino a quando Microsoft non decise di rilevare l'operatore di telefonia voip e di cambiarne radicalemente architettura strutturale (cfr. nota al titolo, *supra*) - era ipotizzabile esclusivamente la possibilità di procedere alla captazione del dato fonico a monte o a valle della protezione crittografica, e quindi esclusivamente nella eventualità che si fosse acquisita la disponibilità o il controllo, anche solo da remoto, del personal computer utilizzato dall'utente bersaglio monitorato.

Ciò in particolare, attraverso l'uso di software del tipo *trojan horse*[184] che consentono di acquisire le comunicazioni suddette e di traslarle verso le sale di ascolto delle autorità competenti.

Tale soluzione tuttavia, in quanto approccio tecnologico non convenzionale rispetto ai tradizionali sistemi ed apparati di intercettazione, pone alcuni problemi di natura giuridica nell'ambito del nostro ordinamento processuale penale, nonostante le norme che disciplinano la materia delle intercettazioni telefoniche, ambientali e telematiche (artt. 266 e segg. c.p.p.) non entrino nel merito della individuazione delle modalità, delle procedure e delle soluzioni attraverso le quali è possibile procedere alle intercettazioni e, apparentemente, lasciano quindi aperta la possibilità di avvalersi di ogni risorsa resa disponibile dall'evoluzione della tecnologia, purché autorizzata dall'autorità giudiziaria.

Gli applicativi del tipo *trojan horse* si comportano, in vero, come una sorta di microspia informatica, ma in realtà si tratta di software che devono essere installati, in locale o da remoto, sul personal computer monitorato per consentirne l'acquisizione dei contenuti dall'esterno, oltre a rendere possibile il monitoraggio delle attività dell'utente.

---

[183] Tali obblighi sono oggi disciplinati, in Italia, dall'art. 96 del d.lgs. 1° agosto 2003, n. 259 (Codice delle comunicazioni elettroniche) e dall' art. 132 del D.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), così come da ultimo modificati rispettivamente dal D.lgs. n°70 del 28 maggio 2012 e dal d.lgs. 30 maggio 2008, n. 109 di recepimento della Direttiva comunitaria 2006/24/CE.

[184] Cfr. para. 2.2.e), *supra.*

L'invasività di tali soluzioni, connessa alla loro stessa natura, potrebbe quindi incidere negativamente sui requisiti di integrità e genuinità della prova acquisita sul computer monitorato.
Dal punto di vista della legittimazione normativa all'utilizzo di tali soluzioni, appare opportuno richiamare l'esperienza tedesca. Le autorità statuali del Land Nord Reno Westfalia nel 2010 avevano, per legge, autorizzato il largo utilizzo, in sede di inchieste penali, del monitoraggio informatico dei personal computer attraverso il largo ricorso ai *trojan horse*, introducendo per questa via il già esaminato concetto di "perquisizione on-line" (cfr. *supra* para. 2.3.e).
Avverso tale provvedimento sono stati avanzati ricorsi alla Corte Costituzionale tedesca che, successivamente, si e pronunciata favorevolmente nei confronti della possibilità di ricorrete a tali approcci intrusivi, ma limitatamente ai casi di terrorismo ed alle situazioni in cui vi è pericolo per la vita umana e la sicurezza nazionale, previa autorizzazione della competente autorità giudiziaria.
E' quindi ipotizzabile che il parlamento tedesco prenda in considerazione la possibilità di introdurre una norma che estenda a livello nazionale tale opzione investigativa.
Nell'esperienza italiana, ad analoghe soluzioni tecnologiche si è fatto ampio ricorso nell'ambito di attività investigative sia di tipo preventivo[185] sia con finalità giudiziarie.
Nel primo caso, evidentemente, non si è posto il problema dell'utilizzabilità degli elementi indiziari o probatori acquisiti con le modalità in questione.
Nella casistica dell'utilizzo dei *trojan horse* in ambito giudiziario, la legittimazione procedurale è stata acquisita mediante l'applicazione dell'art. 266 bis c.p.p., sotto forma di estensione delle modalità tecniche di captazione delle comunicazioni telematiche, già autorizzate dalla competente autorità.
Con riferimento alla questione della possibilità di assoggettare il fornitore della soluzione voip agli obblighi di legge sopra menzionati, si evidenzia infine che talvolta, come nel caso di Skype, il suddetto fornitore non corrisponde al gestore della rete.
Nel caso di Skype, infatti, l'infrastruttura di comunicazione, pur basata su reti fisiche, si avvale di un sistema di cooperazione tra gli utenti (*c.d. clients*), ognuno dei quali può contribuire all'esercizio del sistema, in qualità di supernodo, in proporzione alle proprie disponibilità di calcolo e di banda. La comunicazione tra A e B non procede cioè punto-punto, ma viene disarticolata in una infinità di pacchetti che, previa loro cifratura, viaggiano sulla rete in modo assolutamente randomico attraversando differenti (e numerosissimi) nodi di smistamento costituiti dai singoli utenti che sono in quel momento connessi al client skype e che, inconsapevolmente, mettono a disposizione degli altri utenti una porzione sufficientemente limitata della propria banda e delle proprie risorse di rete.
Il sistema in questione, inoltre, prevede sia un'architettura *peer to peer*, nella quale gli utenti comunicano tra loro esclusivamente su rete IP, tra personal computer, sia

[185] Ai sensi dell' art. 226 delle norme di attuazione, di coordinamento e transirorie del c.p.p., di cui al d.lgs. 28 luglio 1989, n. 271. Cfr. anche para. 1.3.f), *supra.*

una soluzione ibrida, che consente comunicazioni tra utenti della rete telefonica tradizionale (fissa e mobile) e utenti su rete IP.
E' quindi evidente in tale scenario la difficoltà di identificazione dei soggetti ai quali è possibile attribuire la qualità di *operatori di servizi di comunicazione*, indispensabile per l'applicazione della normativa in materia di prestazioni obbligatorie e *data retention*.
A tal uopo, circa la specifica possibilità di considerare skype quale soggetto destinatario degli "obblighi di prestare" contemplati dal codice delle comunicazioni, a prescindere da qualsivoglia disquisizione di ordine giuridico in ordine alla possibilità o meno di includere il fornitore del più famoso servizio voip tra gli "*operatori di servizi di comunicazione accessibili al pubblico",* basti quanto riportato in una mail ricevuta dallo scrivente nel corso del dicembre del 2012 a firma della dottoressa Donatella Proto, dirigente del Ministero dello Sviluppo economico e responsabile della Direzione Generale per i servizi di comunicazione elettronica e radio diffusione che, a tal proposito, così si esprimeva: *"Skype non soggiace ad alcun obbligo ex art. 96 in quanto non è titolare di alcuna autorizzazione per reti e/o servizi di comunicazione elettronica in Italia"*[186]*.*
Nella prospettiva, infine, dell'adozione, da parte della pubblica amministrazione, dei sistemi di comunicazione Voip, qualora tale tecnologia venga implementata quale nuova opzione tra i servizi resi dalle preesistenti infrastrutture di rete, si ripropone il problema suindicato, in quanto all'ente gestore della rete non può evidentemente essere attribuita la qualità di operatore, ai sensi della vigente normativa.

3.1.f) La prima volta che si pone in Italia il problema della intercettazione del voip. Un caso pratico emblematico: il sequestro dell'imprenditore Roveraro[187].

Questi i fatti in estrema sintesi. Nel 2006 a Milano, Il pm della Direzione distrettuale Antimafia Margherita Taddei, insieme agli investigatori che la supportano nell'ambito di delicate indagini di criminalità organizzata si accorgono che alcuni indagati hanno escogitato un modo apparentemente sicuro ed impenetrabile per parlare tra di loro senza correre il benché minimo rischio di essere intercettati: via Skype.

---

[186] In questo senso si veda altresì quanto riportato dal I comma dell'art.40 del codice delle comunicazioni: *"Gli operatori possono negoziare tra loro accordi sulle disposizioni tecniche e commerciali relative all'accesso e all'interconnessione*. *L'operatore costituito in un altro Stato membro che richiede l'accesso o l'interconnessione nel territorio nazionale non necessita di un'autorizzazione ad operare in Italia, qualora non vi fornisca servizi o non vi gestisca una rete. L'Autorità anche mediante l'adozione di specifici provvedimenti garantisce che non vi siano restrizioni che impediscano alle imprese accordi di interconnessione e di accesso.*

[187] Le informazioni riportate in questo paragrafo sono state tratte da un articolo di stampa pubblicato da Repubblica: *"boss e intercettazioni",* Mensurati – Tonacci (15 febbraio del 2009) oltreché dagli atti delle indagini (ormai di dominio pubblico) custoditi negli archivi del Raggrupamento Operativo Speciale (ROS) Centrale dell'Arma dei Carabinieri con sede a Roma.

Il pm, dunque, incarica due consulenti dalle comprovate capacità e conoscenze tecniche di risolvere il problema. Questi contattano i vertici di Skype i quali fissano loro un bizzarro appuntamento: a Londra, in una saletta riservata dell'aeroporto. La società è estone con sede in Lussemburgo. Non c'è motivo di incontrarsi a Londra. I due tecnici tuttavia accettano. La riunione si dimostra, però, alquanto inutile. Il pm decide allora di rivolgersi ad Eurojust. Viene fissato un secondo incontro, stavolta a Milano. Da una parte gli investigatori e la rappresentanza italiana di Eurojust, dall'altra due uomini di Skype: Kurt Sauer (security manager) e Stephen Collins (legale). Gli italiani propongono una serie di soluzioni, sia legali sia tecniche. I delegati della società estone (si ripete, con sede legale in Lussemburgo), però, non battono ciglio, ripetendo quella che di qui in avanti diventerà sempre la «Versione di Skype»: *«Non possiamo per problemi tecnici e non possiamo per problemi giuridici. La normativa del Lussemburgo non ce lo permette»*. La rappresentanza italiana di Eurojust non si rassegna e organizza un terzo incontro, stavolta all'Aja. Da una parte gli investigatori italiani (magistrati delle Dda di Milano e Napoli, guidati dal procuratore nazionale antimafia Pietro Grasso), francesi, tedeschi, inglesi e greci, dall'altra i rappresentanti di Skype. Chi era presente a quella riunione racconta di un clima strano: *«Gli investigatori continuavano a proporre soluzioni, quelli di Skype ascoltavano in silenzio»*. Poi il colpo di scena. *«I lavori erano programmati fino alle 19, ma alle 15 quelli di Skype spariscono nel nulla. Qualcuno sostiene usciti dal retro».* Fine dell'incontro. Lo scontro si arroventa, con i magistrati che continuano a chiedere una mano per le loro indagini e Skype a opporre le solite *«questioni tecniche e giuridiche»*, talvolta utilizzando anche insistenti *"incomprensioni linguistiche*" col chiaro intento di fare ostruzione.
Così, a distanza di solo pochi mesi, l'assenza di espedienti utili all'intercettazione delle comunicazioni skype[188] evidenzia i potenziali risvolti drammatici di una simile impossibilità pratica.

Il 6 luglio 2006 veniva infatti sequestrato a scopo estorsivo Gianmario Roveraro noto finanziere dell'interland Milanese. La vittima veniva messa in comunicazione con i propri familiari mediante alcune telefonate effettuate all'indirizzo della linea residenziale della propria abitazione. Dai tabulati telefonici acquisiti nel corso delle indagini però si poteva constatare che le telefonate fatte dal Roveraro ai familiari (sull'utenza domestica) non presentavano alcun numero chiamante quale identificativo.
Allo scopo di identificare gli autori del reato mediante "geolocalizzazione digitale", personale del Reparto Tecnico del Reparto Operativo Speciale Centrale dei Carabinieri effettuava i seguenti accertamenti:
- preliminarmente veniva ipotizzato che le chiamate in parola potessero essere state effettuate mediante utilizzo di un sistema voip. Ora, tra i servizi voip esistenti e

[188] Almeno fino a quando Microsoft non intervenne a mutarne architettura ed algoritmi (cfr. nota 176 *supra*).

disponibili nella rete Internet in quegli anni, il più diffuso e all'uopo considerato più sicuro era effettivamente Skype;
- veniva pertanto inoltrata all'indirizzo della società Skype formale richiesta tesa ad ottenere i dati rilevanti per l'individuazione dei rei - fermo restando che, trattandosi di una società di diritto Lussumburghese, sarebbe stata necessaria una rogatoria internazionale, con evidenti conseguenti aggravii e pericoloso dispendio di tempo.
Cionondimeno, Skype era stata da poco acquisita dalla società Ebay, la quale, invece, presentava una componente italiana con sede in Milano. Le richieste relative ai tabulati di traffico in questione venivano pertanto rivolte alla società capogruppo Ebay.
Dette richieste vertevano principalmente sull'identificativo delle telefonate in entrata sul numero dell'abitazione della vittima (nelle quali era la vittima stessa ad interloquire con i propri familiari al fine di impartire disposizioni circa la movimentazione finanziaria necessaria per pagare i due milioni di euro richiesti come riscatto).
Ottenuto il richiesto riscontro dalla società E-bay, gli operatori di polizia giudiziaria procedevano all'analisi dei dati forniti. Dagli accertamenti esperiti emergeva la creazione di due utenze sul servizio Skype (*account*), aventi entrambe come identificativo pseudonimi riferibili al cognome della vittima. Entrambe le utenze, inoltre, avevano effettuato chiamate verso il numero residenziale della vittima nella data e nell'orario preso in esame dagli investigatori. I parametri di registrazione delle due utenze erano stati peraltro creati all'inizio del 2005, cioè più di un anno prima della data del rapimento, comprovando, quindi, una lunga progettazione del piano criminoso. Per l'attivazione delle utenze, al momento della sottoscrizione, erano stati forniti indirizzi e-mail aventi, anche'essi, come pseudonimo (*nickname*), termini assonanti col cognome della vittima del sequestro[189].
Dall'esame dei tabulati di connessione forniti da Skype, gli inquirenti venivano inoltre a conoscenza dei numeri IP[190] associati di volta in volta alle utenze Skype. I gestori del servizio di telefonia mobile che avevano garantito la connettività alla Rete Internet all'utente del servizio Skype, attestavano invece l'utilizzo di due schede telefoniche, entrambe intestate ad una prostituta rumena non più reperibile e probabilmente rientrata in patria[191].
La ricerca di altre possibili connessioni alla rete attraverso ulteriori utenze telefoniche (fisse o mobili) rivelava la presenza di una terza ed ulteriore scheda telefonica mobile (SIM Card) anch'essa intestata alla prostituta rumena e che, con le summenzionate utenze telefoniche, andava a creare un "network comunicativo chiuso". Ed in effetti

[189] La richiesta da parte di Skype di un indirizzo email è motivata dalla necessità di intraprendere una corrispondenza con l'utente relativamente a fatturazione delle chiamate o altre comunicazioni di servizio.

[190] Numerazione assegnata all'utente al momento della connessione ad Internet. Si potrebbe considerare l'indirizzo IP come una sorta di targa temporanea assegnata all'utente per poter usufruire dei servizi della Rete. Sul concetto di IP vedi più diffusamente il para 4.2.a) *infra*.

[191] La Romania sarebbe entrata a far parte dell'Unione Europea solo un anno dopo, nel gennaio 2007.

le tre utenze mobili comunicavano solo tra di loro creando per questa via una rete chiusa.

Dall'ulteriore analisi dei dati forniti dal gestore Skype, emergeva inoltre che, in data precedente al sequestro, era stata effettuata una connessione a quel medesimo profilo skype, mediante l'utilizzo di un IP statico che risultava assegnato all'Autorità Europea per la Sicurezza Alimentare (EFSA[192]) di Parma. Venne quindi appurato che presso l'EFSA era presente una rete wi-fi che, senza alcuna protezione di accesso, poteva essere agevolmente raggiungibile anche dall'esterno della struttura.

Ulteriori numeri IP di connessioni (effettuate con i medesimi cellulari[193]) ai servizi a pagamento di Skype, risultarono invece attestati su differenti paesi (per cui una richiesta rogatoria, vista l'urgenza di intervenire, avrebbe comportato il decorso di un eccessivo arco temporale). La particolarità delle predette connessioni lasciava peraltro intuire l'utilizzo di un qualche sistema di "anonimizzazione"[194] in quanto la stessa utenza Skype appena connessasi con un IP serbo, dopo solo pochi minuti, trasmigrava su un IP assegnato da un gestore di connettività russo.

Al fine di asseverare l'effettivo transito economico, relativo all'importo del riscatto, da un conto all'altro, i criminali avevano altresì sottoscritto, utilizzando carte di credito prepagate anonime, un servizio di e-fax. Quest'ultimo si concretizza in un ulteriore servizio fornito in internet da società che ovviano alla necessità di avere un telefax attraverso la creazione di una casella di posta elettronica che, avendo una numerazione virtuale, può inviare e ricevere fax sotto forma di *files* PDF.

I files di *log* relativi alle connessioni al menzionato servizio elettronico di fax, rivelavano - anche in questo caso come conseguenza dell'utilizzo di applicativi di "anonymizer" - la presenza di numerazioni di IP che non garantivano il rintraccio degli autori delle operazioni di connessione.

I sequestratori, in altri termini, al fine di far perdere le proprie tracce in Internet, avevano operato nel seguente modo:

---

[192] L'Autorità Europea per la Sicurezza Alimentare, EFSA, acronimo di *European Food Safety Authority*, è un'agenzia dell'Unione europea istituita nel gennaio del 2002 con sede in Italia, a Parma. Fornisce consulenza scientifica e una comunicazione ufficiale in materia di rischi, esistenti ed emergenti, associati alla catena alimentare.

[193] Univocamente individuati mediante codici IMEI.

[194] L'anonimizzazione è quella attività di mascheramento, durante una connessione internet, dell'IP Ciò avviene prevalentemente mediante l'utilizzo di connessioni cifrate del tipo VPN (*virtual private network*). Le reti VPN – che sono reti private (aziendali ad es.) che sfruttano, ai fini di risparmio economico, un sistema di trasmissione pubblico già esistente (internet appunto), al fine di realizzare i collegamenti necessari fra i vari utenti privati (dipendenti o clienti) - utilizzano collegamenti che necessitano di autenticazione in modo da garantire l'accesso ai soli utenti autorizzati; per garantire la sicurezza che i dati inviati in Internet non siano intercettati o utilizzati da altri non autorizzati (ed infatti il grande vantaggio/pericolo di una VPN è dato dal fatto che sfruttando la rete pubblica deve interagire necessariamente con l'esterno e può quindi anche accedere al web), le reti utilizzano sistemi di crittografia.
Poco prima che il *provider* riceva una richiesta di collegamento dalla VPN (cifrata appunto), la richiesta passa al servizio di anomizzazione che la decodifica e, tramite *proxy* (cioè un programma che si interpone tra il *client* ed il *server* del *provider*), la maschera ed assegna un nuovo IP (quello appunto di anomizzazione) di modo che il provider è soltanto in grado di visualizzare il mero scambio di dati senza che sia in grado di decifrarli e di ricostruirne con certezza l'origine.

avevano innanzitutto creato degli account-utenti di Skype mediante connessioni UMTS effettuate con schede telefoniche (sim) prepagate intestate a prestanomi (la prostituta rumena) ed installate in c.d. Connect Cards[195] (apparecchiature che consentono di appoggiare la connessione dati di un PC ad una rete telefonica mobile); tutte le connessioni effettuate erano state operate mediante sistemi di *proxing* o anonimizzazione al fine di "occultare" il proprio IP. Tuttavia, quest'ultima operazione era stata automatizzata da un programma che, in alcune casi, non aveva assolto al compito prefissato facendo emergere taluni numeri IP attestati su schede prepagate che pertanto furono agevolmente rintracciate; e per finire, erano state effettuate sporadiche connessioni sfruttando la rete WiFi, non protetta, involontariamente fornita dalla EFSA.
Al fine di rintracciare i responsabili del sequestro, gli inquirenti decisero allora di localizzare, mediante l'ausilio dei gestori di telefonia mobile, la sim ancora connessa alla rete telefonica e, mediante l'utilizzo di attrezzature particolarmente sofisticate, riuscirono a georeferenziare ed esattamente localizzare uno degli autori del reato per poi così risalire agli altri correi.
Ciononostante, gli inquirenti non furono in grado di scongiurare il peggio e, nonostante l'intenso lavoro profuso, si scoprì che Gianmario Roveraro era stato brutalmente ucciso proprio durante il suo primo giorno di prigionia per mano di uno dei sequestratori che, così disse, nutriva nei confronti dello stesso forti risentimenti in virtù di un pesante torto subito dalla vittima nei mesi precedenti.

3.1.g) La ricostruzione fonetica delle conversazioni Voip.

Si è visto come uno dei principali ostacoli di carattere tecnico che si frappone alla concreta possibilità di sottoporre ad intercettazione le conversazioni che avvengono in formato digitale (attraverso il ricorso a tecnologia voip – soprattutto ove ciò avvenga attraverso la modalità *peer to peer*) sia costituito dal ricorso, da parte degli operatori, a sistemi (proprietari) sempre più sofisticati di crittazione dei pacchetti che, sottoforma di dati digitali, trasmettono veri e propri messaggi vocali.
E' proprio sotto questo aspetto che merita di essere (per lo meno) menzionato uno studio estremamente interessante condotto e pubblicato, congiuntamente, da un gruppo di ricercatori del Dipartimento di Scienze Informatiche e del Dipartimento di Linguistica dell'Università della North Caroline[196].
La tesi di partenza del lavoro proposto dai ricercatori nordamericani è che lo standard voip rimarrà per i prossimi anni la più fiorente e sviluppata scommessa economica nel settore delle comunicazioni, registrando tassi di crescita inusitati ed aumentando i suoi utilizzatori assidui (abbonati) fino a raggiungere gli oltre 250

[195] Antesignani degli attuali modem USB per sim card.
[196] White A., Matthews A., Snow K., Monrose F., Phonetic reconstruction of encrypted Voip conversation, in Security and Privacy Simposium, maggio – giugno 2011.

milioni di utenti entro l'anno 2013 (nel solo mercato americano!). E se la diffusione del voip crescerà in modo esponenziale, non è altrettanto pacifico che l'attenzione per la sicurezza seguirà di pari passo la sua costante espansione, derivando, dalla precedente considerazione, una forte preoccupazione per le insidie che la tutela della privacy e della segretezza subiranno nell'immediato futuro.

Gli scienziati americani fanno d'altra parte notare come gli attuali sistemi di crittazione (a prescindere da ciò che vogliono lasciar intendere i portavoce di Skype quando parlano di assoluta impossibilità tecnica di sottoporre ad intercettazione le conversazioni tra i loro *clients, cfr. supra)* presentano almeno 2 aspetti di intrinseca debolezza, rappresentati: dall'utilizzo di *codec*[197] VBR (*variable bits rate*) per la criptazione della voce, e dal costante ricorso a flussi di codici che comunque conservano e preservano la lunghezza delle singole parole. Queste 2 circostanze interagiscono fra di loro nell'esporre a rischi di disvelamento una data conversazione voip. Più precisamente, gli acuti ricercatori, attraverso operazioni matematiche più o meno complesse, riescono agevolmente a risalire (dalla mera analisi del flusso di dati criptati) alla lingua parlata, al sesso dei soggetti che comunicano e finanche all'uso di frasi ricorrenti (e note!) fra gli utenti della conversazione voip.

Il metodo utilizzato consiste nel "segmentare", attraverso precise operazioni matematiche e di linguistica computazionale, il flusso di pacchetti di dati (criptati) in specifiche sottosequenze ciascuna delle quali corrisponde ad un dato fonema della lingua parlata dagli interlocutori. Una volta fatto ciò, grazie all'ausilio di un computer opportunamente programmato, applicando le regole e i modelli del linguaggio e del discorso, si risale ad una trascrizione fonetica (anche solo parziale, ma sufficiente a trarre successivi inferimenti) della conversazione.

Lo studio si basa su una analisi assai approfondita delle modalità di funzionamento e delle differenti caratteristiche dei più moderni *codec* utilizzati dai vari sistemi voip. Detta analisi viene poi interfacciata con nozioni di linguistica computazionale, fonetica ed informatica avanzata.

E' vero peraltro che trascrizioni condotte sulla base delle sequenze procedimentali sopra descritte - allo stato dell'arte – molto difficilmente potrebbero entrare a far parte della dialettica dibattimentale ed è assai improbabile che possano essere in grado di concorrere alla formazione della prova in giudizio, almeno fino a quando non si fossero sedimentate in seno alla *computer forensics* regole certe di elaborazione e ricostruzione delle conversazioni voip intercettate nell'originale forma qui presa in esame.

D'altra parte, ciò non esclude che siffatte inedite intercettazioni potrebbero in futuro servire all'inquirente, nella fase delle indagini preliminari, quali atipici spunti investigativi da utilizzare e sviluppare per suffragare ovvero accantonare più ampie ed articolate ipotesi ricostruttive dei fatti.

---

[197] In elettronica, informatica e telecomunicazioni un codec è un programma o un dispositivo che si occupa di codificare e/o decodificare digitalmente un segnale analogico (tipicamente audio o video), affinché possa essere salvato su un supporto di memorizzazione, richiamato per la sua lettura o riproduzione oppure trasmesso a distanza su un canale di comunicazione.

Quali che siano gli sviluppi futuri di tali peculiari tecniche di decifrazione (*alias* intercettazione) delle conversazioni voip, le stesse meritano ad ogni modo di essere menzionate nell'ambito di questo lavoro se non altro perché mostrano – a prescindere da ogni affermazione di segno opposto da parte di chi abbia interesse ad evidenziare l'inviolabilità di un determinato sistema informatico – come nel settore delle tecnologie digitali ed informatiche, nulla è definitivamente impossibile ed ogni ostacolo di ordine tecnico è sempre comunque destinato ad essere rimosso o superato.

Capitolo IV: le investigazioni digitali (approccio “empirico”).

***

“Life is
what happens to you while you’re busy making other plans”
(Lennon J.)

4.1 Considerazioni preliminari.

4.1.a) Premessa.

Come si è sottolineato più volte in precedenza, lo sviluppo delle reti - ed in particolare di Internet - ha determinato grandi opportunità di crescita in campo sociale, economico, politico, culturale e scientifico, fino a ridisegnare gli scenari del nostro vivere quotidiano. La rivoluzione informatica e telematica peraltro ha investito (com’è naturale) anche il mondo giuridico richiedendo ripetutamente l'intervento del legislatore in ogni suo settore, dal diritto civile a quello amministrativo, dal diritto del lavoro a quello - qui di precipuo interesse - penale.
Se però la globalizzazione delle nuove forme di comunicazione ha comportato significativi e tangibili benefici per la società, allo stesso tempo, ha manifestato potenzialità negative altrettanto ampie: la Rete, in tutte le sue possibili applicazioni e forme di utilizzo, è infatti strumento di particolare efficacia per la commissione di condotte criminali alcune delle quali, solo pochi anni fa, del tutto sconosciute ed inimmaginabili.
Con quest'ultimo capitolo, si cercherà quindi di completare la ricerca spostando l'indagine su un piano diverso: si abbandonerà cioè la teoria dei testi in favore di un approccio quasi esclusivamente “empirico” tentando, quindi, di rielaborare e di dare sistemazione logica, oltreché giuridica, ai tanti dati ed alla variegata casistica frutto della lunga esperienza maturata sul campo dagli operatori di polizia[198] nella loro quotidiana attività di prevenzione e repressione del crimine informatico.

4.1.b) Prevenzione e repressione del crimine informatico: gli organi di polizia.

Tutte le volte in cui si fa riferimento al concetto di "criminalità informatica" si ricorre inevitabilmente ad un’immagine dai contorni assai sfumati e non meglio definiti, indicando, con una sola espressione, una molteplicità di condotte criminose

[198] Dei quali fa parte lo scrivente nella sua qualità di ufficiale dell’Arma dei Carabinieri.

lesive dei più diversi beni giuridici: reati contro il patrimonio, contro la riservatezza e la libertà individuale, contro la proprietà intellettuale e via discorrendo. Probabilmente ciò avviene in quanto la tecnologia rimane pur sempre un mezzo neutro, uno strumento cioè che, in quanto tale, può essere orientato tanto allo sviluppo ed al progresso quanto all'offesa e alla lesione delle più disparate posizioni giuridiche altrui.

Alla luce dei pericoli e dei rischi che la Rete e, più in generale, i nuovi sistemi di comunicazione portavano con sé, già all'inizio degli anni '80, si è provveduto ad adeguare convenientemente le strutture investigative degli organi di polizia conformandole alle mutate esigenze e creando, nel corso degli anni, unità sempre più specializzate nel contrasto dei fenomeni criminali caratterizzati dall'utilizzo di apparecchiature ad alto contenuto tecnologico e di avanguardia.

Nacque così nel 1981, con la legge di riforma della Polizia di Stato, la Polizia Postale e delle Telecomunicazioni, originariamente deputata alla tutela del servizio postale e dei servizi di telecomunicazione, ma che negli anni ha visto orientare il proprio campo di azione anche nei settori delle comunicazioni radio, televisive, telefoniche, telematiche e satellitari, così connotandosi sempre più come una vera e propria Polizia delle Comunicazioni.

In realtà, già a partire dai primi anni '90, si erano ben comprese le potenzialità che gli strumenti di alta tecnologia potevano offrire alle organizzazioni criminali, tanto che presso la Direzione Centrale della Polizia Criminale fu creato, proprio in quel periodo, un team di specialisti con compiti di studio ed analisi dei fenomeni criminali legati al settore delle comunicazioni con particolare riguardo alle attività illecite svolte in seno alle grandi associazioni di stampo mafioso.

Nel 1996 l'attività di questa equipe di esperti è stata allargata e generalizzate estendendola al più ampio settore del contrasto ai crimini commessi nel settore delle telecomunicazioni, dando vita al Nucleo Operativo di Polizia delle Telecomunicazioni. La creazione di questo Ufficio è stato il preludio di una vasta riorganizzazione di tutta la Specialità: con decreto del Ministro dell'Interno del 31 marzo 1998, è stato creato il Servizio Polizia Postale e delle Comunicazioni[199] all'interno del quale sono confluite le risorse del N.O.P.T. e della Divisione Polizia Postale. L'articolazione attuale prevede

[199] In relazione all'elevato tecnicismo richiesto dalle attività nella rete Internet e per evitare confusioni e duplicazioni di indagini in una materia così delicata e complessa come quella della pedofilia *online*, la **legge n. 269 del 1998** *("Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù"*) affida, **in via esclusiva**, rispetto ad ogni altro ufficio o servizio di Polizia Giudiziaria, al Servizio di Polizia Postale e delle Comunicazioni, quale organo del Ministero dell'Interno deputato alla sicurezza delle comunicazioni ed al contrasto dei crimini informatici, alcuni specifici poteri e strumenti investigativi. In analogia con quanto stabilito dalle normative a contrasto del traffico di droga e di armi, per la repressione della diffusione di immagini pedopornografiche su Internet e del turismo sessuale, il Servizio ha facoltà esclusiva (previa autorizzazione dell'Autorità Giudiziaria): 1) di effettuare acquisti simulati di materiale pedopornografico; 2) di "navigare" nella rete Internet con agenti sottocopertura; c) di realizzare siti di copertura (c.d civetta); d) di organizzare operazioni con agenti infiltrati, partecipando ad iniziative di turismo sessuale. Vengono, inoltre, previsti, specifici strumenti processuali quali: 1) il differimento dell'esecuzione di atti di polizia giudiziaria altrimenti obbligatori, come il sequestro e l'arresto; 2) la confisca e l'affidamento delle cose sequestrate agli uffici di polizia procedenti.

quindi una struttura centrale, costituita appunto dal Servizio Polizia Postale e delle Comunicazioni, incardinato all'interno della Direzione Centrale della Polizia Criminale (in Roma). Mentre la Direzione Centrale sovrintende ai servizi delle singole Specialità della Polizia di Stato (Stradale, Ferroviaria, Postale, di Frontiera e dell'Immigrazione), il Servizio Polizia Postale e delle Comunicazioni presiede al supporto e al coordinamento dell'attività operativa di 19 Compartimenti regionali (localizzati nelle principali città italiane) e 76 Sezioni provinciali, contando su un organico di circa 2000 agenti.

Giusto per avere un'idea di come opera ogni singolo Compartimento, se ne indica, di seguito, la struttura tipo. Esso è generalmente suddiviso in tre squadre ciascuna delle quali svolge la propria attività d'indagine in specifici settori della criminalità informatica. La prima squadra si occupa di hackeraggio, pedofilia, crimini connessi all'utilizzo illecito di carte di credito, reati di diffamazione e truffe. La seconda squadra lavora sul territorio occupandosi di reati comuni e di illeciti legati alla duplicazione abusiva di software, cd musicali o, comunque, a forme di violazione della legge sul diritto d'autore. La terza squadra si dedica alla pirateria satellitare, alla pirateria del software in Rete, verifica licenze ed autorizzazioni radioamatoriali (cosiddetti CB), degli Internet point, delle videoteche e controlla gli esercizi che commercializzano materiali o apparecchiature di telecomunicazione soggette a marcatura o a omologazione.

L'indagine informatica, va debitamente aggiunto, non è peraltro prerogativa esclusiva della Polizia di Stato[200], ma è un settore sul quale concentrano le proprie attività anche altre forze dell'ordine, come Carabinieri e Guardia di finanza. In particolare, presso quest'ultimo organismo, è stato istituito nel luglio 2000 (anche se è operativo solo dal gennaio 2001) il Gruppo Anticrimine Tecnologico (GAT). Il Gruppo ha un campo d'azione particolarmente ampio investendo tutti i settori in cui viene impiegata la tecnologia per commettere reati: da Internet al telefono cellulare, fino ad arrivare ai sistemi di pay TV. Il coordinamento delle attività della Polizia delle Comunicazioni col GAT avviene sempre tramite la Direzione Centrale della Polizia Criminale di Roma.

Comun denominatore rispetto a tutte le forze di polizia è la specifica metodologia di reclutamento delle risorse umane. La selezione del personale viene effettuata infatti secondo criteri di particolare rigore che tengono conto dell'esperienza investigativa maturata, dei corsi universitari seguiti e delle provate competenze manifestate nel campo dell'informatica e delle telecomunicazioni. In tal modo si può fare affidamento su personale aggiornato, altamente qualificato ed in possesso di specifiche conoscenze tecnico-giuridiche.

4.1.c) il crimine informatico: *a-territorialità* del fenomeno.

[200] Salvo che per le attività di contrasto alla pedo-pornografia, cfr. non precdente.

La minaccia criminale nel mondo virtuale, si distingue nettamente da quella tradizionale primariamente per il suo connaturale superamento delle classiche categorie di spazio e di tempo. La condotta delittuosa, ad esempio, può concretizzarsi in più azioni svolte in tempi diversi o contemporaneamente, da più soggetti o da uno solo, in luoghi diversi o in uno spazio virtuale dalla accentuata evanescenza circa la sua dimensione geografica; tale condotta, inoltre, il più delle volte innesca più processi elaborativi e/o di trasferimento di informazioni che passano, in tempi lunghi o in tempo reale, attraverso spazi indeterminati e spesso indeterminabili; possono essere colpiti immediatamente o a distanza di tempo una o più vittime in uno o più luoghi differenti spesso anche molto remoti e distanti l'uno dall'altro. La velocità con la quale la tecnologia permette di trasferire, alterare o distruggere grandi quantità di dati e informazioni e, più in generale, di portare a termine un crimine, nonché la *a-territorialità* del fenomeno che può assumere una connotazione transnazionale svincolandosi dai confini dei singoli Stati, rappresentano i limiti più gravi alla persecuzione di tali forme di offesa.

Questo perché nel *cyberspazio* i tradizionali confini degli Stati nazionali, se vengono azzerati durante l'azione informatica posta in essere dal soggetto agente, riaffiorano successivamente laddove si tenti di ricostruire il percorso a ritroso alla ricerca delle tracce digitali eventualmente lasciate dall' autore.

La diffusione a livello mondiale della Rete e la virtuale scomparsa del *locus commissi delicti* ha creato e continua a generare gravi problemi di determinazione della competenza territoriale, di giurisdizione nonché di norme applicabili laddove vengano coinvolti più paesi e conseguentemente più organi investigativi e diverse forze dell'ordine.

Ad ogni modo, oggi – quale uniforme protocollo operativo diffuso in tutte le Procure della Repubblica italiane - se un crimine è commesso tramite un *server* situato all'estero, viene tempestivamente data comunicazione della notizia di reato all'Interpol[201] - che prosegue per conto suo le indagini - e alla procura competente per territorio (ove determinabile). Quest'ultima verifica, eventualmente, dove risiede il *server* e inoltra (entro le successive 24 ore) apposita comunicazione all'autorità giudiziaria estera. Se il sito risiede sul *server* di un dato paese, ma è registrato presso un altro Stato, la comunicazione della Procura verrà effettuata ad entrambe le autorità giudiziarie. Esistono, peraltro, numerosi – potremmo definirili - *"paradisi legislativi in materia cybernetica"*, come le Isole Samoa, le cui norme e legislazioni non permettono alcuna forma di intervento anche nel caso in cui i server allocati

[201] L'Interpol, o Organizzazione Internazionale di Polizia Criminale (OIPC), si articola in una struttura centrale ed una struttura periferica, quest'ultima è rappresentata dagli Uffici Centrali Nazionali. In Italia tale unità è collocata in seno al Servizio per la Cooperazione Internazionale di Polizia, posto alle dipendenze della Direzione Centrale della Polizia Criminale. L'Interpol ha il compito di: 1) assicurare e sviluppare la più ampia assistenza reciproca tra le Autorità di polizia criminale, nel quadro delle leggi esistenti nei diversi Paesi e nello spirito della Dichiarazione Universale dei Diritti dell'Uomo; 2) costituire e sviluppare ogni tipo di organismo in grado di contribuire efficacemente alla prevenzione ed alla repressione dei reati di diritto comune.

all'interno del loro territorio ospitano siti che sono al centro di pericolosi fenomeni criminali.

4.1.d) Le dinamiche inerenti la denuncia del crimine informatico.

Se, da un lato, buona parte degli interventi della Polizia delle Comunicazioni è promossa da specifiche richieste di singoli utenti (aziende o privati cittadini), dall'altro emerge un dato piuttosto significativo: una notevole discrepanza tra gli attacchi ai sistemi informatici statisticamente rilevati/denunciati (di numero relativamente esiguo) e quelli effettivamente portati a termine (in numero assai accentuato). Alla base di questo fenomeno vi sono diverse ragioni. Innanzitutto, può accadere che il soggetto colpito non sappia neppure di essere tale, non si accorga, cioè, di essere stato vittima di un'aggressione informatica. Chi commette l'illecito può essere un esperto del settore e, trattandosi, come spesso avviene, di un soggetto interno all'azienda, può essere a conoscenza di informazioni preziose, di tipo tecnico o organizzativo, che lo pongono in una situazione tale da impedire o prevenire qualsiasi rilevamento esterno. In questa ottica, un ruolo cruciale potrebbe essere svolto da una adeguata politica di sicurezza interna, contenendo o limitando la responsabilità di security manager impreparati - che devono, tra l'altro, aggiornarsi costantemente data la rapidità con la quale vengono sfruttate debolezze e falle dei sistemi e protocolli di comunicazione - ma anche la responsabilità del personale dipendente che può far saltare, per ignoranza o dabbenaggine, anche la più sofisticata predisposizione di misure di garanzia (basti pensare ai famosi *post-it* presenti sui monitor o sulle scrivanie che riportano, in bella mostra, *login* e *password* di accesso).

E' singolare peraltro come in alcuni casi (neppure tanto sporadici!), è stata riscontrata nei sistemisti - sia di enti pubblici che di aziende private - una qualche forma di riluttanza nel considerare l'attacco subito come un fatto di reato e ciò, in particolare, quando l'illecita intrusione (*c.d. hacking*) non provoca danni apparenti. Normalmente, quindi, i predetti episodi sono sottovalutati e tollerati, considerati alla stregua di semplici bravate (o al limite di pericoli scampati). Tuttavia, in questi casi, spesso ci si trova davanti a veri e propri attacchi prodromici alla realizzazione di ulteriori reati di ben più rilevanti entità e dannosità. Pertanto, in ipotesi consimili, il sottovalutato accesso abusivo al sistema informatico o telematico (contemplato e sanzionato perltro dall'art. 615 ter c.p. *cfr. supra* para. 2.2.c)). seppur non ha causato alcun danno apparente, potrebbe essere facilmente utilizzato dall'autore (criminale) come "ponte" per entrare in altri sistemi, reali bersaglio ed oggetto di operazioni di cancellazione di dati o di altre condotte criminose.

Ora, se è vero che l'ipotesi delineata, ex art. 615 *ter* co.1 è perseguibile a querela della persona offesa, è altrettanto vero che quasi sempre il fatto è connesso con l'illecita acquisizione dei file di password, condotta che integra, come visto *supra*, il reato di cui all'art. 615 *quater* c.p. (*"Detenzione e diffusione abusiva di codici di*

accesso a sistemi informatici o telematici") procedibile invece d'ufficio. Ciò impone peraltro l'obbligo (almeno per i sistemisti di enti pubblici o incaricati di svolgere pubblici servizi) di denunciare i fatti ai sensi dell'art. 331 c.p.p.[202], obbligo penalmente sanzionato ai sensi degli artt. 361 e 362 c.p. in caso di omissione[203].

D'altra parte, si deve tener presente che a volte le aziende colpite preferiscono non ricorrere alla querela/denuncia perché il fatto di aver subito un attacco è indice di vulnerabilità e, quindi, dal punto di vista del marketing, una cattiva presentazione per clienti attuali e potenziali. Il prezzo da pagare per la pubblicità del fatto può essere troppo alto quando in gioco ci sono reputazione e credibilità aziendali. Questo fenomeno interessa soprattutto certi tipi di imprese commerciali come banche, istituti finanziari, compagnie assicurative, società quotate in borsa, imprese specializzate in sicurezza informatica ecc. ecc., in altri termini tutti quei soggetti per i quali l'offerta di "sicurezza" costituisce una componente essenziale dell'attività esercitata. È un dato acquisito, inoltre, che, per la maggior parte di tali aziende, il ricorso alla magistratura non rappresenta il più delle volte una soluzione neanche a fronte di ricatti o estorsioni posti in essere da vere e proprie organizzazioni malavitose.

Accanto al cosiddetto "danno di immagine", un altro elemento può inoltre trattenere le aziende dalla denuncia: il timore di una responsabilità penale, nonché civile per eventuali danni cagionati a terzi. Deve essere chiarito, però, che in caso di attacco ad un sistema informatico, tali responsabilità sono solo quelle disciplinate dalla normativa sul trattamento e la tutela dei dati personali. La "legge sulla privacy" (art. 31 d. lgs.vo n°196 del 2003) prevede, infatti, l'obbligo giuridico per il responsabile del trattamento di adottare specifiche misure necessarie alla sicurezza dei dati, l'omissione delle quali (sia dolosa, sia semplicemente colposa) è sanzionata penalmente ed amministrativamente[204]. In base, poi, alla predetta legge, chiunque cagioni un danno ad altri per effetto di un trattamento non consono di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. Il trattamento di dati personali è quindi attività considerata "pericolosa" e comporta un'inversione dell'onere della prova (è il gestore a dover provare di *"aver adottato tutte le misure idonee a evitare il danno"*, art. 2050 c.c.).

Va sottolineato, d'altra parte, come sia in pratica facile sottrarsi alle suddette responsabilità: la legge richiede, infatti, la predisposizione di misure di sicurezza "minime" (per non dire ovvie e in alcuni casi anche ingenue ed ampiamente consolidatesi nella prassi di tutti gli operatori). Dette misure, individuate dagli artt. 33 e ss. del codice sul trattamento dei dati personali, consistono peraltro,

---

[202] Art. 331 c.p.p.: *"I pubblici ufficiali e gli incaricati di un pubblico servizio che, nell'esercizio o a causa delle loro funzioni o del loro servizio, hanno notizia di un reato perseguibile d'ufficio, devono farne denuncia per iscritto ... senza ritardo al pubblico ministero o ad un ufficiale di polizia giudiziaria"*. Diversamente rispondono dei delitti previsti dagli artt. 361 e 362 c.p.p. per "omessa denuncia di reato". Ex art. 333 c.p.p., il privato "che ha notizia di un reato perseguibile d'ufficio può farne denuncia. La legge determina i casi in cui la denuncia è obbligatoria".

[203] Si tratta, rispettivamente, dei reati di omessa denuncia di reato da parte di pubblico ufficiale ovvero di un incaricato di pubblico servizio

[204] Artt.31, 33,162 co.2 bis, 169 del codice privacy.

fondamentalmente, nell'adozione di in un sistema di "codici identificativi" (password) per l'accesso al sistema e nell'impiego di idonei programmi di crittazione ed antivirus la cui efficacia ed aggiornamento debbono essere verificati con cadenza periodica.

4.1.e) Il crimine informatico e la volatilità degli elementi probatori

Un altro elemento che non può certo essere trascurato è che nel cosiddetto cyberspazio, anonimato ed omologazione sono attributi che qualificano gli utenti virtuali e facilitano l'occultamento di prove reali e le identità personali dei soggetti che vi operano. Per questa ragione, nell'attività repressiva dei *computer crimes*, la collaborazione dei gestori dei servizi di telecomunicazione, dei servizi internet (Internet Service Provider), dei fornitori di connettività e degli altri operatori in campo è un elemento imprescindibile se si vogliono ottenere risultati concreti. La professionalità del personale impegnato nelle indagini deve essere supportata, soprattutto nella fase di acquisizione delle fonti prova, dalla collaborazione fattiva di tali soggetti nonché delle stesse vittime. Diversamente, la volatilità degli elementi probatori determina situazioni la cui complessità difficilmente potrebbe trovare soluzione.

La prova informatica o elettronica (la c.d. *digital evidence*, cfr. para 2.3 *supra*) è infatti connotata da due intrinseche caratteristiche: fragilità e immaterialità. Le tracce elettroniche sono fragili in quanto facilmente alterabili, danneggiabili e distruttibili. La fragilità della traccia elettronica è congenita ed intrinseca appunto; prescinde dunque da ipotetiche manipolazioni dolose ma finanche, in alcuni casi, da eventuali comportamenti colposi posti in essere da chi interviene su di esse. La perdita casuale di dati è infatti talmente frequente da porsi come problema cogente che necessita di soluzioni *ad hoc* (la sola accensione di un computer spento o l'apertura di un file comporta infatti l'aggiornamento automatico dell'orario di accesso compromettendo quello precedente, così come il mancato utilizzo di un text editor nella fase di copiatura può compromettere la genuinità del testo originario).

L'acquisizione dei dati presso gli Internet Service Providers si inquadra peraltro nel più ampio e complesso tema della *"data retention"* (o *"data preservation"*) e in tale vasta cornice deve essere collocata ogni sua disamina scientifica, con un modello di analisi cioè che integra le questioni tecniche proprie della materia informatica e telematica, con quelle più strettamente giuridiche.

L'acquisizione dei dati presso l'ISP, invero, può essere compiuta in maniera più corretta e consapevole se vi è la conoscenza di tutte le fasi di emivita dei dati stessi e delle procedure di loro acquisizione e osservazione, le quali, con un buon margine di approssimazione, possono essere riassunte in: "generazione", "conservazione", "acquisizione" e "analisi".

La puntuale conoscenza di ciascuna delle suddette fasi porta, in primo luogo, alla presa d'atto dell'esistenza di un certo grado di rischio di alterazione e volatilità dei dati nell'intera filiera e, conseguentemente, della necessità di adottare una serie di

cautele ai fini di preservare la genuinità e la non "ripudiabilità" delle informazioni raccolte[205].

In particolare, l'identificazione di un soggetto, di un luogo o di eventuali tracce di reato, che costituiscono atti tipici di polizia giudiziaria, sono, in questo settore, essenzialmente riconducibili al cosiddetto IP Address, dal quale si può (spesso solo tentare di) risalire, attraverso particolari accertamenti tecnici, a soggetti fisici[206].

La circostanza infatti che ad ogni connessione ciascun *client* (postazione) sia contrassegnata da un IP Address unico al mondo (per quella sessione), non esclude tuttavia che l'identificazione e la localizzazione dei singoli elaboratori collegati alla rete sia in qualche modo resa più difficoltosa (se non impossibile) dall'utilizzo di *software* in grado di occultare l'identità della macchina grazie alla quale ad esempio si è portato l'attacco ad un sistema informatico, ovvero da cui è partito un messaggio a contenuto diffamatorio.

È poi possibile imbattersi in interventi che abbiano comportato la cancellazione *ad hoc* dei *file* di *log* al termine delle operazioni illecite condotte sui sistemi attaccati, cosicché sarà vano tentare di ricostruire a ritroso i vari "passaggi" compiuti dal sistema, così come anche risalire all'utenza telefonica dalla quale è partita la connessione nel corso della quale è stata consumata la condotta penlmente illecita.

Tra i più diffusi sistemi di "occultamento" dell'identità dei sistemi informatici utilizzati per scopi illeciti vi è quello della creazione di siti web denominati *"anonymous remailer"*, che consentono la cancellazione dei dati elettronici dell'utente (rendendone di fatto impossibile l'identificazione) mediante la rimozione e sostituzione delle informazioni concernenti appunto la provenienza del mittente di una qualsiasi comunicazione. E' così possibile nascondere, per esempio, l'identità dei mittenti dei messaggi di posta elettronica, inducendo il *server* di posta a sostituire l'intestazione del mittente, ed a inviare il messaggio al destinatario con intestazioni fittizie.

Altro metodo per impedire l'identificazione dell'autore di atti/fatti telematici consiste nella possibilità di cancellazione dei *file* di *log*.

Particolarmente diffuse sono poi diverse tecniche di utilizzo fraudolento degli identificativi dell'elaboratore di un soggetto: in questi casi l'autore del comportamento illecito non soltanto nasconde la propria identità, ma addirittura crea le condizioni perché il comportamento sembri apparentemente attribuibile ad un altro utente davvero esistente. L'*hacker* acquisisce l'identificativo e la password di un utente ignaro, e si collega alla rete sotto mentite spoglie. L'acquisizione dell'identificativo e della password del resto possono avvenire o in via "tradizionale" (riuscendo a carpirne gli estremi direttamente dall'utente mediante azioni di *social engineering*, *infra*), ovvero acquisendole per via telematica attraverso l'uso di quei specifici programmi denominati *"trojan horses"*;

---

[205] A tal proposito si veda quanto riferito *supra* in relazione alle problematiche connesse alla *computer forensic* (para2.3.b).

[206] Per questa ragione, spesso, la perpetrazione di reati informatici e non, si focalizza sull'utilizzo di computer appartenenti ad istituti universitari, Internet-Cafè ecc. ecc.

La collaborazione "convinta" degli ISP (fermi comunque restando gli obblighi di legge pendenti su di essi, cfr. para. 1.4.f), *supra*) rimane dunque cruciale proprio perché tutto sembra, di fatto, ruotare intorno all'*IP Address*, elemento, questo, fondamentale per "tracciare" ed individuare anche il più astuto tra i criminali informatici.
Va infine ricordato come l'indirizzo IP sia contenuto proprio in quei famosi *file di log* la cui conservazione (per un certo periodo) non è prevista come obbligo di legge a carico degli ISP per ciò che concerne i *contenuti web* "visitati" dal sospetto (a differenza di ciò che è invece prescritto per le società telefoniche le quali, al contrario, sono tenute a conservare i c.d. dati esterni relativi alle utenze telefoniche chiamate: quali numero identificativo del chiamato [oltreché del chiamante], durata della conversazione, celle d'appoggio, ecc. ecc. cfr. para 1.4.e) *supra*).

4.1.f) segue: i *files di log*[207].

Per risalire all'autore dell'illecito, dunque, è sovente determinante acquisire i *file* di *log*. Occorre in proposito chiarire che esistono diversi *file* di *log*, ciascuno deputato alla registrazione di particolari attività svolte dall'utente sulla o tramite la macchina alla quale ha ottenuto l'accesso. I *file* di *log* che qui interessano, sono quelli (memorizzati sul server dell'ISP) che contengono i dati relativi all'inizio e alla fine di una sessione di navigazione di uno specifico utente (collegatosi con un certo *username* e una certa *password*), nonché, soprattutto, l'indirizzo IP del computer (indirizzo assegnato dal server stesso) che ha richiesto l'accesso alla Rete. Una volta acquisiti, tali file vengono confrontati con i tabulati telefonici e permettono così di risalire all'intestatario della linea chiamante. È su quest'ultimo che, in primo luogo, ricadrà la responsabilità per l'uso illecito del computer.
Merita d'altra parte di essere ulteriormente sottolineato quanto già enunciato precedentemente[208]: nessuna legge prevede l'obbligo di conservare i *file* di *log* relativi ai contenuti dei siti web visitati (diversamente da quanto è invece previsto per la posta elettronica). Inoltre, l'obbligo di consegna degli stessi scatta per l'ISP solo a fronte di un decreto motivato del pubblico ministero[209], ma tali *file*, si badi, potrebbero anche non avere alcuna efficacia probatoria stante la loro intrinseca natura di semplici *file* di testo facilmente soggetti ad alterazione senza l'adozione di specifiche cautele[210].

---

[207] Quanto riportato in questo paragrafo deve essere necessariamente integrato con quanto riferito *supra* ai para 1.4.e) e 1.4.f).
[208] Para 1.4.e) *supra.*
[209] Salvo quanto diversamente previsto da talune norme speciali come quelli in materia di lotta al terrorismo internazionale cui all'art. 5 della L. n°431 del 2001.
[210] Al fine di garantirne l'inalterabilità, i file potrebbero, per esempio, essere cifrati con un algoritmo crittografico (apposizione di sigilli digitali analoghi a quelli apposti su porte, buste o contenitori).

Data la più volte rievocata volatilità degli elementi probatori, in caso di qualsivoglia illecito informatico bisogna agire tempestivamente informando, nel più breve tempo possibile, l'Autorità giudiziaria e/o la Polizia Giudiziaria e fornendo loro tutte le indicazioni utili alle indagini. In particolare, gli inquirenti, come prima cosa, il più delle volte, si procureranno i relativi *file* di *log* in ordine:

1. agli accessi (data, ora, durata connessione, IP assegnato, *hostname* ed eventuale *caller ID* - numero chiamante);

2. alle attività svolte nel sito, *mail*, *newsgroup*, *ftp*, ecc. (sempre con data e ora);

3. alle attività *proxy* (consente di verificare le pagine http).

Gli investigatori, inoltre, cureranno che gli orologi di macchina siano esattamente sincronizzati, al fine di evitare discrepanze casuali con gli orologi di sistema.
Inoltre, nel caso specifico di **illecita intrusione in un sistema protetto** da misure di sicurezza, le informazioni che sarebbe opportuno rendere all'Autorità Giudiziaria sono:

a. tipo e versione del sistema in uso (hardware e software);

b. tipo di sicurezza utilizzata e modalità di applicazione;

c. ogni *file* di *log* che riporti traccia di accessi indebiti e i riferimenti dei *timing* di macchina;

d. i nominativi delle figure professionali di riferimento tecnico (ove esistano);

e. descrizione della tipologia di *networking* e della relativa architettura funzionale nonché nomenclatura delle interconnessioni in rete geografica o locale;

f. descrizione particolareggiata del tipo di operazioni illecite accertate e dello stato delle cose dalle quali si evince la tipologia delle operazioni accertate;

g. in base alle operazioni accertate, occorre fornire quanti più elementi di verifica delle stesse;

h. descrizione particolareggiata delle modalità attraverso le quali si è pervenuti alla conoscenza dell'illecita intrusione;

i. informazioni relative a indicazioni giunte da terzi dei fenomeni trascorsi o in corso;

j. informazioni relative a indicazioni rese a terzi dei fenomeni trascorsi o in corso;

k. in caso di intrusione senza danni, ma con acquisizione del *file* di *password*, per i sistemisti di Enti Pubblici (pubblici ufficiali e/o incaricati di pubblico servizio) vi è l'obbligo di denuncia ex art. 331 c.p.p., mentre tale obbligo non sussiste per i privati;

l. indicare i nominativi delle persone che possono essere informate dei fatti;

m. prima di ogni azione, al momento della scoperta dell'illecito, occorre eseguire un *backup* delle sole *directory* e/o *file* interessati dalle modifiche/alterazioni o contenti informazioni relative all'attacco: in caso di modifica al file di *password*, salvare il file modificato prima di rimpiazzarlo.

L'attività di raccolta ed analisi dei *file* di *log* va considerata, quindi, propedeutica e preparatoria rispetto alla (eventuale) fase di indagine successiva che, il più delle volte, soprattutto nei casi che destano maggior allarme e preoccupazione, passerà attraverso l'instaurazione ed effettuazione di mirate intercettazioni telematiche ai sensi dell'art. 266 bis c.p.p.
Per l'identificazione dell'autore del reato, spesso, occorre inoltre procedere alla perquisizione dell'abitazione o dell'azienda presso cui è installata l'utenza da cui è partita la connessione illecita, con il conseguente sequestro dei p.c. e del materiale informatico nella disponibilità dell'utilizzatore.
Allorché si procede a perquisizione, peraltro, specie se l'indagato è soggetto particolarmente esperto nell'uso degli strumenti informatici, è bene disporre con separato provvedimento la temporanea interruzione dell'energia elettrica presso i locali da perquisire, sì da di impedire che durante l'esecuzione dell'atto l'utente/indagato alteri i dati oggetto di ricerca magari intervenendo "da remoto" sul proprio sistema attraverso uno *smatphone* .
Vale la pena di sottolineare inoltre che, ai fini del buon esito delle indagini, le intercettazioni telematiche, non devono essere intese o richieste in quanto tali, ma sempre congiuntamente (preferibilmente) ad un'ordinaria intercettazione telefonica. Nella stragrande maggioranza dei casi, infatti – soprattutto quando ad operare è una organizzazione criminale - ogni scambio di dati o programmi o testi in via informatica è preceduto da conversazioni nelle quali i soggetti interessati si abbandonano (anche solo verbalmente) a commenti o all'indicazione di specifiche tecniche, anche al solo fine di procedere alla inizializzazione delle attrezzature di trasmissione e ricezione dei segnali (settaggio dei modem, velocità di trasmissione, estensione della memoria, caratteristiche della compressione utilizzata e cosi via) e, soprattutto, trattandosi di *password* o programmi abusivamente duplicati, essi si dimostrano ben consapevoli della relativa provenienza illecita o della parimenti illecita destinazione.
In conclusione, giova ancora una volta sottolineare come pure per i *log* valgono le medesime considerazioni che vengono svolte in materia di acquisizione probatoria del dato digitale rispetto all'esigenza di ridurre al minimo il rischio di alterazione. Sempre più spesso, d'altronde, alle lacune derivanti dall'esistenza di norme assai generiche si sommano alcune carenze di specializzazione nel mondo forense.
La questione relativa all'acquisizione dei *log* presso l'ISP, d'altra parte, è priva di significativi riscontri giurisprudenziali. La prassi consolidata peraltro è quella di acquisire i dati formulando una richiesta *ad hoc* direttamente al fornitore, delegando quest'ultimo ad effettuare l'estrazione, la duplicazione e la trasmissione dei dati all'autorità richiedente. È ancora aperto il dibattito circa la natura di tale atto di

acquisizione, e in particolare se esso costituisca un "accertamento tecnico" in senso stretto, e inoltre se lo stesso, in quanto tale, sia ripetibile.
Si tratta evidentemente di questioni di particolare rilevanza (si pensi per esempio all'ipotesi dell'incidente probatorio), le quali possono essere sviscerate se, come si diceva *supra*, si è in grado di conoscere nel dettaglio le modalità tecniche di generazione e conservazione dei dati del traffico. La già citata esigenza di poter contare su modelli e linee guida condivisi nella *computer forensics*, qui emerge in tutta la sua evidenza, laddove si potrebbe auspicare l'adozione di vere e proprie regole tecniche di generazione e conservazione dei dati, utili a garantirne l'immodificabilità.
Si pensi, per esempio, a un delitto informatico commesso nei confronti di un ISP da parte di un suo stesso cliente/abbonato. In quel caso, l'acquisizione dei *log*, nelle modalità consolidatesi nella prassi, sarebbe rivolta direttamente alla parte offesa, in totale assenza di garanzie circa l'integrità dei dati.
Va da se, infine, come l'analisi dei *log* in ambito forense debba essere svolta da operatori adeguatamente qualificati e, stante la mole notevole di dati da esaminare, realizzarsi con l'impiego di specifici strumenti software. Detto esame, peraltro, deve essere scrupolosamente documentato in tutti i suoi singoli passaggi, dando pedissequamente indicazione delle componenti hardware, dei sistemi operativi e dei *tools* (con relative licenze d'uso) utilizzati per raggiungere lo scopo.

4.1.g) segue: notazioni relative al sequestro di dati informatici.

Un'ulteriore notazione riguarda la possibilità di avvalersi con sempre maggiore frequenza, nell'ambito di indagini che abbiano ad oggetto crimini informatici, dello strumento del sequestro preventivo (della linea telefonica/ADSL interessata) onde precluderne la perpetrazione di ulteriori condotte delittuose, ovvero, soprattutto ai fini probatori, del sequestro probatorio dei programmi e delle attrezzature rinvenute in seguito a perquisizione domiciliare.
All'uopo va segnalato che l'art. 253 c.p.p. non è stato oggetto di rivisitazione neppure dopo l'emanazione della legge n°48 del 2008 di recepimento della Convenzione di Budapest, per cui rimane irrisolto, nel nostro ordinamento, il problema della sequestrabilità del dato informatico *ex se*, soprattutto alla luce del fatto che, sempre la L. n.48/08, da un lato, ha abrogato il secondo comma dell'art. 491 *bis* c.p. - che forniva una definizione in un certo senso "fisica" del documento informatico, legandolo strettamente ad un supporto su cui era registrato *("il documento informatico è …il supporto")* – e, dall'altro, non ha recepito la definizione di dato informatico fornito dalla Convenzione di Budapest, se non in maniera indiretta (dando esecuzione cioè all'intera Convenzione).
Il legislatore è invece intervenuto massicciamente sull'art. 254 c.p.p. (sequestro di corrispondenza), riscrivendone il primo comma, con la previsione in capo all'Autorità Giudiziaria di procedere al sequestro presso i fornitori di servizi postali, telegrafici,

telematici o di telecomunicazioni di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica.
La norma in esame pone un problema interpretativo di una certa rilevanza, relativo alla "sequestrabilità" delle *e-mail* e dei messaggi SMS ed MMS.
Il dettato letterale del nuovo art. 254 c.p.p., in effetti, parrebbe consentire siffatta interpretazione, ma trattandosi del contenuto di comunicazioni telematiche pare senz'altro preferibile ricorrere al regime di acquisizione previsto dall'art. 266 *bis* c.p.p., che certamente risulta più garantito dall'intervento del Giudice per le Indagini Preliminari.
È poi stato introdotto un nuovo articolo, il 254 *bis* c.p.p., il quale prescrive che allorquando l'Autorità Giudiziaria dispone il sequestro presso i fornitori di servizi informatici, telematici o di telecomunicazioni dei dati da questi detenuti, compresi quelli di traffico e di ubicazione, può stabilire, per esigenze di regolare fornitura dei servizi medesimi, di acquisire tali dati mediante copia lasciando al fornitore l'onere della conservazione degli originali.
Va rilevato in proposito che la procedura in questione è solo facoltativa e non obbligatoria e che essa non è prevista, forse irragionevolmente, per l'acquisizione di dati informatici anche presso altri soggetti che potrebbero subire gravi disagi in caso di sequestro.
Dalla disamina precedente emerge dunque un quadro in tema di sequestro che poco differisce rispetto al precedente e non risolve i problemi che si sono spesso verificati in passato.
Nella pratica, infatti, specie in considerazione delle scarse risorse a disposizione della Giustizia (la Legge che ha provveduto a dare attuazione alla Convenzione di Budapest non ha previsto oneri per la sua attuazione se non a favore del CNCPI, il Centro nazionale per il contrasto della pedopornografia sulla rete internet), si procede di regola ad ispezione solo in casi rarissimi (in costanza di arresto o quando si tratti di dati conservati presso terzi che non possono fermare la loro attività produttiva, ad es. ISP o banche), mentre nell'ordinaria amministrazione la P.G. e l'A.G. continuano a procedere al sequestro dell'intero materiale di supporto.
D'altra parte, la perquisizione ed il conseguente sequestro probatorio - operazioni effettuate così come prescrive il Codice di Procedura Penale dalla Polizia Giudiziaria su decreto motivato dell'Autorità Giudiziaria - rappresentano, nella prassi di indagine, gli strumenti tipici di ricerca della prova. Ciò peraltro continua a valere pure per l'accertamento di fatti di reato connessi ad Internet, ovvero a condotte criminose commesse mediante l'utilizzo delle nuove tecnologie. A tal proposito, deve essere evidenziata la necessità che tali operazioni siano sempre eseguite da personale particolarmente qualificato. Solo personale specializzato potrà, infatti, individuare quali strumenti e quali dati siano effettivamente rilevanti ai fini dell'indagine e debbano quindi essere oggetto di sequestro[211]. Molto spesso, però, la Polizia Giudiziaria non ha le competenze informatiche richieste e questo, se da un lato potrà

[211] Soprattutto quando il sequestro concerne beni e strumentazioni di proprietà della vittima del reato.

pregiudicare irreparabilmente l'esito delle operazioni stesse, dall'altro potrà, altresì, causare danni ingenti ed inutili alla parte che le subisce.
In questi anni, del resto, non sono mancate critiche che hanno riguardato l'utilizzo (spesso abnorme) del sequestro probatorio e le modalità stesse di svolgimento di singole attività di indagine.
Ci si può riferire, ad esempio, alle critiche (apparse anche su diverse riviste di settore) relative al frequente sequestro di un intero *server* effettuato dalla Polizia Giudiziaria al fine di acquisire, e al tempo stesso impedire, la diffusione di messaggi diffamatori contenuti in un sito *web* ospitato da un *provider*. Critiche legittime se si considera che sarebbe stato, invece, possibile il sequestro e la conseguente rimozione del solo sito interessato o, addirittura, del solo messaggio diffamatorio così da non danneggiare l'attività del *provider* e consentire a tutti gli utenti non coinvolti dalle indagini di continuare ad usufruire dei suoi servizi.
Altro caso frequente di eccessiva invasività - lamentato soprattutto dalle imprese - è quello che si è spesso verificato in presenza di *softwares* illecitamente duplicati ed utilizzati (in ambito infra-aziendale): al fine di acquisire le fonti di prova, infatti, la Polizia Giudiziaria ritiene sovente opportuno, in modo alquanto sbrigativo, sequestrare direttamente il computer (non di rado, comprensivo di monitor e periferiche) sul quale è installato il programma non licenziato. In una situazione del genere sarebbe, invece, di regola sufficiente (dandone atto nel verbale) soltanto riversare il tutto su un altro supporto magnetico e porre sotto sequestro il contenuto dell'hard disk sul quale è installato ed utilizzato il software illecitamente duplicato (limitatamente al sistema operativo utilizzato ed al software incriminato). In questo modo, dopo aver comunque rimosso il software in questione dall'hard disk sul quale alloggiava, diverrebbe possibile lasciare la memoria di massa con tutti gli altri dati in essa contenuti nella disponibilità dell'azienda senza pregiudicarne l'esercizio delle attività, in ossequio ai principi di gradualità, ragionevolezza e proporzionalità della misura .
Peraltro, anche la giurisprudenza, già da diversi anni,sembra assestarsi su posizioni maggiormente garantiste. Così, con un ordinanza abbastanza risalente, il Tribunale del riesame di Torino[212] ha ritenuto, in un caso di diffamazione a mezzo Internet, pienamente fronteggiabili le esigenze probatorie con la sola estrazione di una copia dell'intero contenuto del supporto informatico utilizzato per commettere il reato e ordinato la restituzione immediata dell'hard disk sequestrato al legittimo proprietario ritenendo applicabile il terzo comma dell'art. 254 c.p.p. che dispone, appunto, *"l'immediata restituzione all'avente diritto delle carte e degli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile"*. Ed infatti, ex primo comma dello stesso articolo, è sequestrabile solo la corrispondenza *"che comunque può avere relazione con il reato"*, mentre - così si esprime il tribunale: *"appare altamente verosimile che* (sull'hard disk sequestrato n.d.r.) *vi siano (anche) una serie di e-mail che potrebbero non concernere la fattispecie di reato contestata"*.

[212] Tribunale Penale di Torino Sez. del riesame, Ordinanza del 7/2/2000

Va detto che, dopo i numerosi sequestri che, in passato, dissimulavano una ingiustificabile natura afflittiva/interdittiva, la tendenza più recente è senz'altro nel senso di procedere, ove possibile, alla creazione di copie delle memorie di massa, da analizzare in un secondo momento.

Oggi pertanto, se ad essere sottoposto a sequestro è l'intero computer - sempre che non scatti (o si presuma possa scattare) l'obbligo della confisca prevista come misura obbligatoria dalla recente legge 15 febbraio 2012 n°12 – detto computer, dopo l'estrazione delle copie necessarie - ricorrendo alle modalità approntate dalla *computer forensics* – dovrebbe sempre essere restituito al legittimo proprietario il quale, considerati i tempi sempre estremamente lunghi delle Procure, non subirà (o perlomeno non dovrebbe subire) alcun danno da obsolescenza!

Va infine precisato come la citata legge n°12 del 2012, al pari di tutti gli altri provvedimenti che contemplano prescrizioni analoghe[213], nel disporre la confisca obbligatoria (previo sequestro) di tutti i *"beni informatici e telematici"* pertinenti ai *cybercrime*[214] (ricomprendendo nel novero di detti beni qualsiasi *res* – materiale o immateriale – utilizzata, anche soltanto in parte, per perpetrare reati informatici), prevede anche che la sanzione accessoria non trovi applicazione nei casi in cui detti beni appartengano a terzi estranei ai fatti di reato[215].

Quid iuris, nondimeno, nei casi di truffe poste in essere avvalendosi delle piattaforme informatiche e telematiche di istituti di credito quando le stesse piattaforme siano state, ad esempio, utilizzate per "pescare" (nel caso di c.d. *phishing*) i conti corrente di ignari clienti? In molti di questi casi, infatti, non sarebbe difficile ipotizzare (come pure sovente è avvenuto) una qualche forma di concorso - quantomeno nella forma del concorso omissivo - per non aver impedito l'avverarsi dell'evento criminoso e tale circostanza, a rigore, potrebbe condurre al sequestro (finalizzato alla confisca) anche degli strumenti informatici e telematici delle predette società creditizie, in attesa che si stabilisca se tali società siano o meno "terze" rispetto ai fatti per cui si procede.

Va da ultimo segnalato che la legge n°12 prevede che, nelle more del sequestro, i predetti beni informatici siano assegnati in custodia giudiziaia con facoltà d'uso agli organi di polizia che ne facciano richiesta e che agli stessi (o ad altri enti dello stato che operano nel settore della Giustizia) ne sia assegnata la titolarità definitiva qualora il sequestro si commuti in confisca.

---

[213] Così ad es. in tema di beni confiscati nell'ambito dell'attività di contrasto alla pedopornografia, al contrabbando, al traffico di droga, alla prevenzione e repressione dell'immigrazione clandestina. Parzialmente diverso è invece il caso di confisca nell'ambito di misure di prevenzione patrimoniale ai sensi della normativa antimafia dove si prevede la sequestrabilità ai fini di confisca dei patrimoni mafiosi illecitamente accumulati anche nei confronti degli eredi anche quando questi siano estranei all'attività delinquenziale del dante causa.

[214] La relazione di accompagnamento al disegno di legge n°2271 prevede che le norme in esso contenute debbano trovare applicazione esclusivamente nell'ambito dei reati informatici *stricto sensu,* quelli cioè espressamente previsti dal codice penale, ricomprendendo altresì tra gli stessi le truffe perpetrate attraverso l'utilizzo di strumenti informatici e digitali.

[215] Tipicamente è il caso dei beni (informatici) aziendali rispetto ai reati (informatici) commessi dai dipendenti avvalendosi delle risorse dell'azienda.

4.2 L'Internet Protocol.

4.2.a) *"*Privacy *versus "tracing".*

Giunti a questo punto, occorre precisare ed ulteriormente sviluppare taluni concetti già espressi in precedenza[216] che, soprattutto in un'ottica investigativa, pongono peraltro agli inquirenti non pochi e non secondari problemi di ordine tecnico-operativo.

Il definitivo recepimento mediante il D.lgs.vo n°109 del 2008 della Direttiva 2006/24/CE in materia di *data retention* dimostra, infatti, come i concetti di *privacy* e di garanzia di un'ampia sfera di riservatezza da riconoscersi a tutti soggetti di diritto, vengano, ormai, sempre più spesso anteposti e messi in contrapposizione ad essenziali e spesso centrali esigenze investigative. Quanto appena affermato, d'altra parte, è indiscutibilmente evidente in tema di *cd. tracing*[217] che, come noto, costituisce il primo e basilare accertamento tecnico nell'ambito della stragrande maggioranza delle indagini in materia di cybercrime.

Ancora una volta, peraltro, è necessario intendersi sugli specifici termini adoperati e sullo stesso scenario investigativo del quale si discorre, evitando quella facile confusioni concettuale che induce ad equiparare, *tout court,* una simile operazione di "tracciamento" a quella, apparentemente affine (ma in realtà ontologicamente differente), che è l'attivita di "intercettazione".

Anche perché i risultati del *tracing* non sono altro che un "indirizzo IP" (*Internet Protocol* [218]) di connessione della macchina dalla quale, verosimilmente[219], è partito l'evento informatico costituente ipotesi di reato.

---

[216] Segnatamente ai para 1.4.e) ed 4.1.f).

[217] Con tale espressione ci si riferisce a quel "percorso a ritroso" che permette agli inquirenti di ritrovare l'origine di una condotta criminosa posta in essere avvalendosi di strumenti informatici.

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

[219] Infatti, abbinato a questo IP possiamo trovare: I) un computer isolato, II) un computer in rete (aziendale, wireless), III) un c.d. internet mobile phone (telefoni di ultima generazione, che consentono le connessioni internet) con scheda prepagata quasi sempre aperta (nel caso la si voglia utilizzare per scopi illeciti) con dati apocrifi, nonostante l'art.. 55, comma 7 decreto legislativo 1° agosto 2003, n. 259 (Codice delle comunicazioni elettroniche) prevede che *«tutti gli acquirenti del traffico prepagato della telefonia mobile»* siano *«identificati prima dell'attivazione del servizio, al momento della consegna o messa a disposizione dell' occorrente scheda elettronica (S.I.M.)»*, imponendo altresì alle imprese di adottare *«tutte le necessarie misure affinché venga garantita l'acquisizione dei dati anagrafici riportati su documento di identità, nonché del tipo, del numero e della riproduzione del documento presentato dall'acquirente».* E' questa una norma di evidente importanza anche nelle ipotesi in cui si voglia implementare su quella scheda, *rectius* sul titolare ed effettivo utilizzatore di quella SIM, un servizio di intercettazione (telematica e/o telefonica).

E dunque un (semplice) numero di telefono relativo alla richiesta connessione dal quale - per ovvi motivi – non è possibile automaticamente risalire all'identità personale dell'effettivo utilizzatore di quel computer.
Sennonché, Il c.d. "Gruppo per la tutela dei dati personali - Articolo 29"[220] ha affermato, nel 2002[221], che *«gli indirizzi IP attribuiti agli utenti Internet costituiscono dati personali[222] e sono tutelati dalla direttiva 95/46/CEE e 97/66/CEE».*
Affermare la natura di dato personale[223] di un indirizzo IP non deve trarre però in inganno l'interprete e portarlo ad affrettate conclusioni. Infatti, l'IP è un dato che solo se (ed in quanto) posto in relazione ad altri dati (ovvero: data e ora di connessione) è in grado di restituirci un risultato "potenzialmente" lesivo della riservatezza, dal momento che - in una determinata frazione di tempo - l'Internet Service Provider (ISP) attribuisce quel determinato indirizzo IP ad un (solo) utente intestatario del relativo contratto per la connessione ad Internet. Ma nulla ancora sappiamo di questo utente se non il numero di telefono utilizzato dallo stesso e i dati (c.d. esterni) relativi alla tipologia della intervenuta connessione.
Orbene oggi - come ricordato più volte nei paragrafi precedenti - l'art. 132 d.lgs. 196/2003 (Codice in materia di protezione dei dati personali, c.d. Codice della privacy) - anche alla luce delle ultime modifiche introdotte con il d.lgs. 109/2008 - esclude testualmente che l'obbligo di conservazione riguardi (alla stessa stregua dei dati attinenti alle conversazioni telefoniche) i "contenuti" della comunicazione informatica (a meno che non si ponga in essere una intercettazione).
E' la stessa Direttiva che nell'esplicare le categorie di dati (relativi al traffico telematico) oggetto di conservazione fa espresso riferimento ai soli IP di "origine" della connessione internet, indicando altresì, quanto ai dati (sempre esterni) del "destinatario", solo quelli riferibili alla telefonia (anche via internet) e alla posta elettronica (cfr para 1.4.e) *supra*.
Ed è proprio il Garante per la protezione dei dati personali a rendere ancora più esplicito il concetto (apparentemente) palesato dalla "Direttiva" e lo fa nell'ambito della relazione annuale, relativa all'anno 2008, ove, tra le varie istruzioni, sottolinea: *«i gestori devono infatti conservare esclusivamente i dati di traffico telematico funzionali alla fornitura e alla fatturazione del servizio di connessione e non i dati di*

---

220 Il Gruppo, istituito dall'art. 29 della direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, del GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione. Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una volta. Il Gruppo adotta le sue decisioni a maggioranza semplice dei rappresentanti delle autorità di controllo. Fra i compiti più rilevanti quelli disciplinati dall'art.30 della direttiva: I) esaminare le questioni attinenti all'applicazione delle norme nazionali di attuazione della direttiva; II) formulare pareri sul livello di tutela nella Comunità e nei paesi terzi; III) consigliare la Commissione in merito ad ogni progetto di modifica della direttiva.

221 "Parere 2/2002 sull'uso di identificativi esclusivi negli apparecchi terminali di telecomunicazione".

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

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

traffico apparentemente "esterni" alla comunicazione (pagine web visitate o gli indirizzi Ip di destinazione) e che possono peraltro coincidere di fatto con il "contenuto" della comunicazione, consentendo di ricostruire meglio relazioni personali e sociali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute».

Tuttavia, è proprio detta impossibilità giuridica (non tecnica, si badi) ad accedere agli IP di destinazione a rappresentare, spesso, per gli investigatori un ostacolo insormontabile negli accertamenti in materia di *cybercrime*, trovandosi sovente gli stessi (ad esempio nelle ipotesi di accesso abusivo ad un sistema informatico/telematico) nella necessità di ricostruire "a ritroso" il percorso che ha portato l'autore di un reato informatico a perpetrare i suoi intenti criminali sul *WEB*. E ciò si rende ancor più evidente ove il gestore fornitore di connettività – come oggi sempre più frequentemente accade - faccia uso si sistemi NAT/PAT[224].

Il più delle volte verrà pertanto impedita - in nome della (tutta da dimostrare) tutela di dati di "asserito" carattere personale - una molteplicità di importanti riscontri informatici ad azioni volutamente poste in essere non solo dall'indagato (nella commissione dei reati), ma anche dalla persona offesa (anche al fine di tutela preventiva: si pensi che, senza IP di destinazione, sarà davvero difficile per il medesimo fornire una prova informatica a riscontro di quanto indicato in denuncia).

Peraltro, a ben vedere, in tema di IP di destinazione nulla avrebbe impedito al legislatore italiano di prevedere diversamente - sia pure nei ristretti spazi di manovra lasciati dalla Direttiva - ove si consideri la previsione di cui all'art. 5 non tassativa, ma solamente indicativa di dati *"attinenti al contenuto delle comunicazioni"* (i soli a non poter essere effettivamente conservati ai sensi dell'art. 5.2 della Direttiva).

In altre parole, l'IP di destinazione poteva ben essere considerato come uno dei *«dati necessari per rintracciare e identificare la destinazione di una comunicazione»* (art. 5.b Direttiva), nonostante lo stesso non venga poi espressamente menzionato ai successivi punti 1 e 2.

Una simile soluzione, oltre a cogliere le osservazioni critiche di cui sopra, non avrebbe costituito in ogni caso una lesione alla riservatezza altrui, tenendo conto che neppure tale dato di per sé solo, come ampiamente dimostrato, è in grado di restituire **il** contenuto della comunicazione. Senza omettere di considerare altresì che una simile impostazione della questione avrebbe, in un certo senso, sanato l'inspiegabile discrasia sussistente rispetto alla possibilità di custodire e conservare da parte del gestore telefonico i dati identificativi di destinazione della

---

224 Nel campo delle reti telematiche, il network address translation o **NAT**, ovvero traduzione/traslazione degli indirizzi di rete, conosciuto anche come network masquerading, ovvero native address translation, è una tecnica che consiste nel modificare gli indirizzi IP dei pacchetti in transito (sia di origine che di destinazione) su un sistema che agisce da *router* all'interno di una comunicazione tra due o più *host*. In pratica, un dato indirizzo IP – di origine o di destinazione- cambia fisionomia (e quindi stringa numerica identificativa) durante il suo percorso. Viene detto IP masquerading (a volte NAT dinamico), invece, un caso particolare di *source* NAT (nat di origine), in cui le connessioni generate da un insieme di computer vengono "presentate" verso l'esterno con un solo indirizzo IP. La tecnica è detta anche Port Address translation (**PAT**), IP Overloading o NAPT (Network Address and Port Translation), in quanto vengono modificati non solo gli indirizzi IP ma anche le porte TCP e UDP delle connessioni in transito. Questo metodo prevede di individuare una rete "interna" (che tipicamente utilizza indirizzi IP privati) ed una "esterna" (che tipicamente utilizza indirizzi IP pubblici), e permette di gestire solo connessioni che siano originate da host della rete "interna".

telecomunicazioni (*alias* numeri degli utenti chiamati, da conservare ai fini di giustizia). Forse che l'informazione concernente la chiamata indirizzata ad un particolare numero telefonico (si pensi, solo per rimanere nell'attualità delle indagini informatiche, a numerazioni a tariffazione maggiorata quale un 899 legato a servizi erotici) non possa ugualmente creare un pregiudizio in punto di riservatezza?
E' significativo, d'altra parte, che Il testo di legge di recepimento della Direttiva (d.lgs.vo n°109 del 2008), introduca per il futuro - con la previsione di cui all'art. 3 comma 2 - la possibilità di specificare, ove si renda necessario e pur sempre nell'ambito delle categorie di cui all'art. 3 comma 1 (comunicazioni telematiche), i dati da conservare. C'è da augurarsi quindi che una simile specificazione, idonea a ricomprendere l'IP di destinazione tra i dati da conservare, venga introdotta al più presto, evitando – come spesso avviene nel nostro Paese - che si metta mano alle norme solo dopo il verificarsi di casi concreti che rendano ormai evidenti all'opinione pubblica le lacune legislative esistenti.
Per ragioni di completezza, infine, va anche sottolineato come numerosi Stati dell'U.E. quali: Germania, Repubblica Ceca, Romania, Cipro, Ungheria, Svezia, Grecia, Irlanda e Austria, lungi dall'implementare nel senso sopra descritto le proprie normative in tema di *data retention* (in recepimento della Direttiva 2006/24 EC), abbiano, invece, sin alla radice, espunto dai loro Ordinamenti qualsivoglia possibilità di raccolta e conservazione dei dati esterni relativi alle comunicazioni telefoniche ed elettroniche dei propri cittadini, in quanto ritenute dalla rispettive Corti Costituzionali incompatibili con le libertà democratiche, i principi ispiratori e gli stessi diritti fondamentali garantiti dai singoli assetti nazionali.
Il predetto atteggiamento di (totale) chiusura da parte di un numero tanto cospicuo di Stati appartenenti alla U.E. rispetto alle problematiche di *data retention,* fa emergere, sotto un diverso profilo, una questione estremamente delicata e preoccupante in relazione ad eventuali indagini future nell'ambito delle quali, ad esempio, pericolose organizzazioni criminali e/o terroristiche potrebbero porre in essere attività di proselitismo utilizzando *account* di posta elettronica di società (magari italiane ma) con i propri *server* allocati sul territorio di uno dei predetti Stati.

4.2.b) L'IP come "dato esterno" di una comunicazione elettronica.

L' inquadramento giuridico dell'IP di destinazione quale dato c.d. "esterno" alla comunicazione e quindi non facente parte del "contenuto" della medesima, trova autorevole conferma in una sentenza, emessa nel 2000, a Sezioni Unite dalla Suprema Corte[225] che riafferma la seguente distinzione concettuale: 1) *"intercettazione"* è la captazione di una comunicazione (*rectius*, dei contenuti della intercettazione) in corso ed è ad essa contemporanea; 2) *"acquisizione di un tabulato"* è apprensione di un dato storico che avviene successivamente alla comunicazione.
Con la logica conseguenza che i "dati esterni" alla comunicazione possono essere raccolti (dopo che la comunicazione si è esaurita) sotto forma di documento, con decreto del Pubblico Ministero così come del resto previsto dall'art. 256 c.p.p. (e oggi ribadito dall'art. 2 d.lgs. 109/2008 che ha eliminato il cd. doppio binario di

[225] La già citata Sentenza n°6 delle SS.UU. emessa in data 23.02.2000, Presidente D'Amuri.

acquisizione dei dati del traffico telefonico/telematico, tramite l'abrogazione del comma 2 e 4 dell'art. 132 del Codice in materia di protezione dei dati personali).
Con una chiarezza espositiva ed una lungimiranza senza precedenti, la Corte, in un passaggio della motivazione aggiunge ancora: *«I "tabulati" sono soltanto elementi identificativi esterni al contenuto della conversazione, la cui informatizzazione non li rende estranei alla comunicazione bensì al contenuto del dialogo intercorso. Tale informatizzazione non concerne i flussi in movimento captati nel corso del loro svolgimento, appunto perché è costituita da dati storici di archivio dei quali già dispone il gestore della telefonia indipendentemente dalla richiesta dell'autorità giudiziaria, che ne ordina l'acquisizione con provvedimento motivato, in quanto non liberamente divulgabili, avendo carattere riservato secondo la normativa sulla "privacy" (L. n. 675/96). Pertanto, la stampa e l'acquisizione dei dati esterni incidono sul loro "trattamento", costituendo una forma d'intrusione nella sfera della riservatezza, diversa e minore rispetto all'intercettazione dei contenuti delle conversazioni o dei dialoghi in corso. Tra intercettazione ed acquisizione dei tabulati vi è la stessa differenza che sussiste fra sequestro della corrispondenza per apprenderne i contenuti e sequestro dei registri postali per venire a conoscenza dei dati esterni afferenti alla corrispondenza inoltrata».*
La stessa nozione dovrebbe valere dunque anche per i *files di log* di destinazione da intendersi appunto come una sorta di "tabulati informatici".
Sul punto è intervenuta, incidentalmente, anche la Corte Costituzionale[226] allorquando si è trovata ad affrontare la questione di legittimità costituzionale sollevata dal Giudice per le indagini preliminari di Roma in relazione alla (irragionevole, dal punto di vista del giudice *a* quo) disparità prevista dall'art. 132 Codice *privacy* in relazione al già ricordato regime binario di conservazione/acquisizione dei tabulati telefonici (24/48 mesi).
In quella pronuncia il Giudice delle leggi, esaminando l'ineluttabile esigenza di contemperamento di opposte posizioni egualmente tutelate dalla Costituzione - protezione della riservatezza dei dati personali, da un lato, aspettativa che lo Stato preservi, attraverso il perseguimento in sede giurisdizionale dei comportamenti criminosi, le condizioni essenziali della convivenza civile, dall'altro – aderisce ciononostante all'orientamento prevalente.
D'altra parte - come lucidamente sottolineato da alcuni commentatori - pur potendo attingere a molteplici argomentazioni per elevare il diritto alla protezione dei dati personali al rango costituzionale - fuorviata forse dalla materia telefonica - la Corte Costituzionale ha optato per il solo articolo 15 della Costituzione che, tuttavia, come noto, fa esclusivo riferimento alla diversa nozione di comunicazione (avendo di mira la salvaguardia della segretezza dei suoi contenuti).
Tuttavia, il parallelo con la materia delle intercettazioni telefoniche (rientranti nelle categorie delle "comunicazioni" e come tali tutelate) non è del tutto calzante, vertendo invece il giudizio sulla materia della tutela dei dati personali.
Pertanto è ragionevole rilevare - con riferimento alla *vexata questio* circa la conservazione dei *file* di *log* di destinazione - la mera esistenza di una blanda forma di intrusione nella sfera di riservatezza dei soggetti; un'intrusione peraltro di sensibile minore impatto rispetto a quella che si realizzerebbe qualora a dover essere conservate fossero gli stessi contenuti delle conversazioni/comunicazioni.
Diverso, quanto agli esiti, sarà peratanto il bilanciamento di interessi nei due diversi casi richiamati, ovvero:

[226] Corte Cost.le Sent. 14 novembre 2006, n. 372

a) esigenze di accertamento/prevenzione dei reati (ex artt. 101, 104 e 112 Cost) *vs.* tutela della libertà di comunicazione (attinente ai contenuti della stessa e non già ai meri dati esterni) costituzionalmente garantita ex art. 15;
b) esigenze di accertamento/prevenzione dei reati vs. tutela dei dati personali.

In conclusione, alla stregua delle precedenti riflessioni, risulta davvero difficile sostenere che, nel bilanciamento tra posizioni giuridiche soggettive, la protezione del dato personale possa prevalere sulle esigenze (assolutamente primarie) di accertamento e repressione di fatti oggetto di indagine nell'ambito di procedimenti penali (trattandosi peraltro - pare superfluo ricordarlo - di conservazione di dati per esigenze di giustizia e non certo di business o altro).

4.2.c) L'acquisizione dei dati informatici relativi al traffico: le innovazioni della l. 48/2008 in materia di sequestro.

Con l'introduzione dell'art. 254-bis c.p.p. ad opera della normativa di recepimento della Convenzione di Budapest sul cybercrime, sembra venuto meno un dubbio interpretativo che - all'epoca dell'introduzione dell'art. 132 Codice privacy - aveva suscitato l'interesse dei commentatori più attenti.
Ovvero se la previsione del d.lgs. 196/2003, in punto di acquisizione dei dati relativi al traffico, potesse - sotto tale profilo - costituire uno sbarramento (trattandosi di previsione speciale e peraltro successiva) all'applicazione dell'ordinario strumento del sequestro così come previsto dal Codice di Procedura Penale.
Orbene, è oggi assolutamente pacifico, alla stregua della normativa in disamina, che il Pubblico Ministero[227] dispoga di due strumenti tra loro, non esclusivi, ma semplicemente alternativi.
Con possibilità quindi di ottenere ex art. 254-bis c.p.p. (ove ricorrano i presupposti generali previsti dall'art. 253 c.p.p. ed in particolare il *nesso di pertinenza*) i dati di traffico anche oltre il termine di cui all'art. 132 d.lgs. 196/2003, sempre che gli stessi siano rimasti nella disponibilità dei relativi gestori per le necessità di cui all'(invariato) art. 123 comma 1 e 2 Codice privacy[228], e quindi per un periodo di tempo che - a

[227] Un ulteriore problema (non ancora normativamente risolto ma che, sempre più spesso, si ripropone nel concreto delle aule di Giustizia) è quello della possibilità per il Giudice civile di poter acquisire i dati relativi al traffico, ove utili per risolvere una controversia. Allo stato, infatti, parrebbe sussistere una preclusione normativa (con profili di dubbia costituzionalità, delle previsioni che limitano alla Autorità Giudiziaria penale un simile potere acquisitivo) dal momento che l'art. 132 comma 3 fa espresso riferimento al Pubblico Ministero (o comunque a soggetti che si muovono nell'ambito di un procedimento penale).

[228] Art. 123. Dati relativi al traffico
1. I dati relativi al traffico riguardanti contraenti ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5.
2. Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per il contraente, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale.
3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se il contraente o

seconda delle interpretazioni[229] - può arrivare fino a 10 anni. Negli stessi casi (e cioè oltre i 12 mesi dalla data della comunicazione), sembra oggi ragionevole affermare – proprio alla luce della richiamata introduzione normativa e stante l'abrogazione del comma 4 dell'art. 132 Codice privacy - che il Pubblico Ministero possa comunque sempre acquisirli con "l'ordinario" strumento del decreto motivato ex art. 256 c.p.p.
Del resto, non si vede come possa essere azionato il più invasivo strumento del sequestro dei dati del traffico senza poter invece richiederne la semplice acquisizione, salva comunque - in questa ipotesi e a differenza dei casi ex art. 132 comma 3 d.lgs. 196/2003 - la legittima possibilità del gestore di disattendere la richiesta della Autorità Giudiziaria, attestandone l'intervenuta cancellazione in quanto (allo scadere dell'obbligo di conservazione ex art. 132 comma 1) non più necessari ai sensi dell'art. art. 123 comma 1 e 2 Codice privacy.

4.2.d) I dati relativi alle chiamate VOIP: peculiarità di Skype.

Sul punto l'inciso di cui all'art. 1 lett. d) d.lgs. 109/2008 *(«chiamate telefoniche…(omissis)… basate sulla trasmissione dati, purché fornite da un gestore di telefonia»*) rende manifesta l'interpretazione accolta, per la prima volta in una norma di legge, dal nostro legislatore. La stessa relazione illustrativa è chiara sul punto: *«per quanto riguarda le chiamate effettuate tramite i servizi di telefonia vocale basati sul protocollo internet (VOIP), si è ritenuto che la natura del gestore influisca sulla natura del servizio, per cui il relativo traffico è definito di natura telefonica se lo stesso è fornito da un gestore di telefonia, viceversa, il traffico ha natura telematica qualora il gestore sia un internet service provider»*. Conclude tale relazione che *«ciò rileva naturalmente ai fini della disciplina applicabile relativa al periodo di conservazione dei dati»*. La questione peraltro aspetta una sua più completa risoluzione normativa, soprattutto nell'ambito dell'inquadramento giuridico delle intercettazioni delle chiamate VOIP, che, a ben guardare, poteva essere sicuramente risolta con l'occasione del recepimento della Direttiva.
Per quanto concerne poi la possibilità di "georeferenziare" gli utenti del più noto (e, da quello che risulta, meno violabile) servizio voip, cioè Skype – soprattutto per ciò che concerne le comunicazioni *peer to peer*, quelle cioè che frappongono maggiori

---

l'utente cui i dati si riferiscono hanno manifestato preliminarmente il proprio consenso, che è revocabile in ogni momento.

4. Nel fornire l'informativa di cui all'articolo 13 il fornitore del servizio informa il contraente o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3.

5. Il trattamento dei dati personali relativi al traffico è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30 sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

[229] A seconda che si consideri operante un termine di prescrizione breve ovvero la prescrizione ordinaria.

problemi tecnici (e giuridici) rispetto alla loro intercettazione – va detto che da un'attenta analisi del protocollo comunicativo si è rilevata un'evenienza che potrebbe mostrarsi utile ai fini investigativi e di Polizia Giudiziaria.
Nel momento stesso in cui si connette al Server di Skype (che autorizza l'accesso alla rete di comunicazione proprietaria), l'utente scarica ed aggiorna, di *default,* lo stato *online* della propria *Buddy List* (*alias* lista dei contatti). Contestualmente alla lista degli pseudonimi e dei *nickname*, viene anche attestato lo "stato" dei vari utenti[230]; in termini tecnici questa informazione consta di un *"flag"*, cioè una definizione di stato, corredata da un numero IP. Il numero IP dei contatti comunicati all'utente appena collegatosi è relativo all'ultimo controllo effettuato dalla rete Skype stessa, ed è pertanto suscettibile di modifiche.
Quest'ultimo è il motivo per il quale l'utente, per verificare che il contatto da chiamare sia ancora disponibile a quel numero IP – cioè alle coordinate Internet comunicate dal Server - reitera inconsapevolmente un controllo. Tale operazione tecnicamente complessa va considerata come quella dell'utente che, per maggiore sicurezza, voglia ricontrollare il numero di telefono temporaneamente assegnato ad un suo contatto prima di chiamarlo.
Pertanto, l'utente Skype invia, a sua insaputa, un pacchetto di controllo all'utente da contattare prima di interessare i potenziali Supernodi; il pacchetto di controllo sarà in chiaro (non cifrato) e conterrà il vero IP del destinatario della chiamata.
Questa peculiarità, finalizzata ad un miglior reperimento dell'utente da chiamare, riveste per le attività di indagine, un'importanza enorme permettendo infatti (se non la puntuale individuazione) la geolocalizzazione dell'interlocutore chiamato. Questo comportamento della rete proprietaria Skype, infatti, consente di acquisire, attraverso l'utilizzo di un analizzatore di protocolli gratuito (quale "Wireshark"[231]), il *vero* indirizzo IP e, quindi, le *vere* coordinate Internet dell'utente chiamato, prima che intervenga l'azione dell'ormai ben noto algoritmo di "Elezione del Supernodo" a criptarne i dati.
Ai fini investigativi, il primo utilizzo che emerge dalla situazione innanzi descritta, si concretizza nella possibilità di georeferenziare tutti i contatti di un utente sol che si riesca a venire in possesso delle credenziali di connessione dell'utente monitorato. Una volta ottenuta la connessione al *client* con un *account* "clone", infatti, sarà sufficiente effettuare una chiamata (che viene interrotta immediatamente) per catturare il pacchetto che contiene l'IP dell'utente chiamato (e da georeferenziare). Tale applicazione in particolare potrebbe trovare impiego durante le indagini tese alla ricerca di latitanti ovvero per tracciare e monitorare gli spostamenti di consorterie criminali.

---

[230] Come la maggior parte dei programmi finalizzati alla comunicazione, anche Skype segnala la modalità attuale di connessione dei singoli contatti presenti nella propria rubrica (*assente, occupato, online…*).

[231] *Wireshark* (precedentemente chiamato *Ethereal*) è un software per analisi di protocollo o *packet sniffer* (letteralmente annusatore di pacchetti) utilizzato per la soluzione di problemi di rete, per l'analisi e lo sviluppo di protocolli o di software di comunicazione e per la didattica. *Wireshark* possiede tutte le caratteristiche di un analizzatore di protocollo standard.

Ove fosse poi in corso un servizio di intercettazione ai sensi dell'art. 266 bis del c.p.p. verrebbe addirittura meno, ai fini della georeferenziazione, anche la necessità pratica di procurarsi le credenziali di accesso all'account del soggetto monitorato atteso che i dati in discorso, proprio in virtù del peculiare modo di funzionare di Skype, emergerebbero anche nel corso di un'analisi dei c.d. "dati freddi". Il protocollo di comunicazione di Skype, infatti, presenta un ulteriore singolare comportamento che si manifesta durante l'attività di *log in* (o accesso al servizio). Ogniqualvolta cioè si avvia il programma, questo, prima ancora di procedere alla criptazione dei dati, al fine di accertare la presenza di un possibile aggiornamento del *client software*, invia taluni pacchetti di dati. Questa attività (che una volta attivato il *client* Skype ha la priorità su tutte le altre) è facilmente visibile usando massima cura nell'analisi delle connessioni emerse in sede di intercettazione. Si dovranno pertanto ricercare gli accessi eseguiti su "ui.skype.com" - univoco sito per la manutenzione degli aggiornamenti del software di Skype – e procedere alle stesse medesime operazioni illustrate precedentemente per il reperimento delle coordinate Internet dell'interlocutore partendo dal pacchetto di verifica inviato all'indirizzo dell'IP del chiamato.

4.3 La "notitia criminis"[232].

4.3.a) La vittima del reato informatico

Nel nostro ordinamento processual-penalistico, la vittima (o persona offesa) di un qualsivoglia tipo di reato è generalmente un attore ancillare, non determinante e non qualificante la legittimità del processo.
Parte civile, al più con funzioni di stimolo ad una astratta efficacia del processo penale (sempre che il costo di esserci valga la pena!).
Eppure la vittima è - di regola, nell'articolato mondo del *cybercrime* - l'istanza principale da cui generalmente prende le mosse l'indagine. Costituisce la principale prova del fatto che un *vulnus* al legame sociale è stato inferto e, come si diceva poc'anzi, rappresenta la fonte usuale della *notitia criminis*, anzi, nella stragrande maggioranza dei casi, la sua volontà, è precondizione stessa della azione penale.
Con troppa frequenza, tuttavia, accade che la vittima sia presto resa muta dalla distanza, dai tempi dell'attività requirente e, soprattutto, da quelli (eccessivamente lunghi) del processo e dei diversi gradi del giudizio.
Ridotto ad attore irrisolto e marginalmente utilizzato (salvo che per le necessarie informazioni preliminari), spesso gli resta solamente l'eventuale umana sensibilità di un operatore della giustizia, di Polizia o, più raramente, del PM che lo rendono in, qualche modo, partecipe allo svolgersi della vicenda procedimentale.

[232] Si richiamino, altresì, le considerazioni svolte *supra* ai para 4.1.d), 4.1.e) e 4.1.f).

Quanto detto sopra, peraltro, in materia di reati informatici, induce sovente la persona che ha visto ricadere sulla propria individualità gli effetti dell'azione delittuosa, addirittura, ad omettere di comunicare alle autorità preposte l'offesa subita e, rifugiandosi nelle *mailing list*, nei *forum* o più frequentemente nei *social network*, cerca di sfruttare, a sua volta, le potenzialità offerte dall'informatica per dar voce alla propria frustrazione e per rispecchiarsi senza mediazione alcuna nelle altre vittime dei medesimi reati ottenendo, per questa via, riconoscimento e solidarietà.
Ora, l'importanza di un costante monitoraggio da parte degli organi inquirenti di detti "spazi" di aggregazione nel *web* (per lo più aperti od accessibili previa semplice registrazione), è facilmente desumibile dal fatto che è spesso proprio grazie all'esame dei vari interventi, discussioni e *post* sui precedenti *media* che possono essere appresi fatti, eventi e notizie circostanziate costituenti ipotesi di reato (trattandosi frequentemente anche di delitti perseguibili d'ufficio) che altrimenti rimarrebbero del tutto sconosciuti ed ignoti a coloro che, istituzionalmente, sono chiamati a prevenire e se del caso reprimere la perpetrazione di reati informatici.
In definitiva, un'attività di "prossimità" alle vittime oltre a farle sentire meno sole ed inadeguate – condizioni che inducono a trovare rifugio, come detto, in soluzioni di *self help* - ne promuoverebbe un ruolo decisamente più attivo finanche nel reperimento dei primi elementi probatori ovvero nel recuperare le tracce fondamentali da cui muovere l'indagine.

4.3.b) La gestione della *notitia criminis*.

La specificità delle condotte e delle problematiche afferenti ai c.d. *computer crimes* ha indotto talune Procure della Repubblica[233] a dotarsi di modelli procedurali e protocolli organizzativi che, nelle migliori intenzioni di chi li ha ideati, dovrebbero essere preordinati a realizzare sinergie più strette e più spediti canali di comunicazione tra Polizia Giudiziaria e PM competenti a trattare i singoli fascicoli riguardanti episodi di *cybercrime*.
Orbene, uno degli aspetti procedurali che ha maggiormente premuto verso una riorganizzazione delle metodologie riguarda, com'era prevedibile, la fase iniziale delle indagini, quella cioè immediatamente successiva all'acquisizione della *notitia criminis* ad opera della Polizia Giudiziaria. Il riferimento puntuale su cui si è cercato in particolare di attirare l'attenzione è il termine temporale entro cui deve avvenire la trasmissione della comunicazione di notizia di reato (contraddistinta dagli addetti ai lavori con il semplice acronimo CNR).

[233] Per quanto concerne, ad esempio, la Procura della Repubblica di Milano – una delle meglio organizzate in fatto di gestione e trattazione dei fascicoli in tema di *cybecrime* – si veda Caiani F., D'Agostino D.,Vannin W.,*"Di necessità, virtù": appunti per una strategia globale al contrasto del cybercrime. l'esperienza del pool reati informatici della procura di Milano*, in IISFA Memberbook 2011 DIGITAL FORENSICS a cura di G. Costabile e A. Attanasio Condivisione della conoscenza tra i membri dell' IISFA ITALIAN CHAPTER.

Ai sensi dell'art. 347 c.p.p.: *"acquisita la notizia di reato, la polizia giudiziaria senza ritardo riferisce al pubblico ministero, per iscritto, gli elementi essenziali del fatto e gli altri elementi sino ad allora raccolti, indicando le fonti di prova e le attività compiute, delle quali trasmette la relativa documentazione".*

L'indicazione temporale ("senza ritardo"), introdotta dalla novella del 1992 al posto delle originarie "quarantotto ore" - che lascia oggi alla Polizia Giudiziaria un maggior margine di autonomia operativa - merita un duplice approfondimento.

Ed infatti, considerati i ristretti termini di conservazione dei dati (cd. *data retention, cfr. supra*) oggi in vigore, è quanto mai opportuna una celere trasmissione della CNR al fine di ottenere l'idoneo provvedimento di acquisizione presso i gestori di comunicazione dei dati relativi al traffico telematico, ad opera del Pubblico Ministero.

Si tratta, in ogni caso, di trovare un giusto contemperamento tra esigenze contrapposte: infatti, se da un lato il problema sopra indicato è di effettiva portata pratica, dall'altro è frequente che alla acquisizione della mera *notitia criminis* possano (anzi, debbano) seguire alcuni accertamenti volti ad acquisire i primi riscontri investigativi per autonoma iniziativa della Polizia Giudiziaria (come detto sopra, è lo stesso art. 347 c.p.p. a richiederlo).

E dunque un ritardo nella trasmissione della comunicazione di notizia di reato sarà da considerarsi ingiustificato – ed in tal senso passibile di sanzioni[234] - solamente ove lo stesso sia stato, in quanto eccessivo, tale da pregiudicare la stessa persecuzione del reato.

Tutto ciò premesso e stante l'esponenziale aumento del flusso di fascicoli riguardanti la specifica categoria di reati in materia di *cybercrime*, presso gli uffici di molte Procure capoluogo, si è ritenuto opportuno, in un'ottica di riorganizzazione del lavoro, elaborare - accompagnato da un dettagliato prontuario esplicativo (continuamente aggiornato) delle più moderne metodologie di approccio alle singole ipotesi delittuose - una classificazione della tipologia di casi ogni giorno affrontati di competenza degli istituiti *pool* reati informatici.

Si è visto, infatti, come una pronta individuazione della categoria di appartenenza - accompagnata dalla standardizzazione degli schemi e delle procedure di "gestione" dei singoli casi - siano utili per meglio porre in essere, ad opera della Polizia Giudiziaria, gli accertamenti minimi di volta in volta richiesti, propedeutici e preliminari rispetto alla trasmissione della comunicazione della notizia di reato.

D'altra parte, una pronta individuazione (a monte) della categoria di appartenenza di ogni singolo caso è utile agli stessi Uffici di Procura dal momento che – a fronte di un sensibile aumento di comunicazioni di notizie di reato in materia informatica – è fondamentale, per il buon esito della loro trattazione, porre mano ad una adeguata organizzazione del lavoro a partire da schemi standardizzati condivisi con la Polizia Giudiziaria medesima.

[234] Sanzioni sia disciplinari (art. 16 disposizioni di attuazione c.p.p.) sia penali (art. 361- 363 c.p.).

È evidente il senso di simili *tandem* frutto di condivisi protocolli investigativi: la casistica ha infatti ampiamente dimostrato che solo le informazioni adeguatamente ed efficacemente raccolte e prontamente comunicate, in maniera strutturata ed organizzata, all'Autorità Giudiziaria territorialmente competente, portano a risultati investigativi congrui e tendenzialmente remunerativi.

4.3.c) I problemi di giurisdizione.

Come si accennava *supra* (para 4.1.c), nel *cyberspazio*, i tradizionali confini nazionali degli Stati, se vengono azzerati durante l'azione informatica posta in essere dal soggetto agente, riaffiorano successivamente, in tutta la loro problematicità, laddove si tenti di ricostruire il percorso a ritroso alla ricerca delle tracce digitali eventualmente lasciate dall'autore.

Di conseguenza, il più delle volte, gli investigatori che si imbattono in notizie di reati informatici (e correlative indagini) che presentano profili di "estraneità"[235], si vedono costretti, di volta in volta, a richiedere agli Stati interessati, ai fini della ricerca della prova (digitale), una adeguata collaborazione tramite formali richieste di assistenza giudiziaria. Inoltre, accade assai di frequente che le stesse società che forniscono i servizi di comunicazione elettronica e che hanno i server in altri Stati, il più delle volte si dichiarino disposte ad una collaborazione che sia la più completa e celere possibile, salvo poi paventare e, successivamente, palesare non sempre chiari ostacoli giuridici promananti da normativa interne ai singoli Stati.

D'altra parte il Consiglio d'Europa, padre della Convenzione del 2001 sul *cybercrime*, già da tempo si è avventurato sui nuovi percorsi dettati dall'evoluzione tecnologica, affrontando i profili attinenti alla giurisdizione e alla necessità di una più stretta collaborazione con i fornitori di servizi di comunicazione elettronica quali unici detentori - molto spesso - delle evidenze informatiche utili ai fini investigativi.

In tale nuova ottica l'imperativo categorico non è più quello dell'attuazione, bensì quello dell superamento e dell' implementazione della Convenzione di Budapest[236].

Tornando al problema in precedenza adombrato, va aggiunto che, in relazione alla collaborazione da offrirsi da parte dai gestori dei servizi di comunicazione digitale, due sono le principali (contrapposte) impostazioni.

Da un lato, quella che privilegia il dato obiettivo del luogo di allocazione dei *server* interessati, spesso al di fuori degli Stati Membri dell'Unione Europea (è il caso assai frequente delle grandi *corporation* americane quali Google, Yahoo e Microsoft). Questa opinione dogmatica arriva a sostenere che, non essendoci server sul territorio

---

[235] A volte poiché le società fornitrici del servizio di comunicazione elettronica hanno provveduto a registrarsi presso un paese estero, ovvero per la materiale dislocazione in un paese terzo dei loro server.

[236] Fra i tanti si da qui atto, a scopo indicativo, di un importante documento elaborato nell'ambito del Consiglio d'Europa ed approvato ai margini della *Octopus Interface – Cooperation against Cybercrime*, tenutasi a Strasburgo nell'aprile del 2008: *"Guidelines for the cooperation between law enforcement and internet service providers against cyber crime"* su cui cfr. para. 4.5.c) *infra* .

nazionale o comunque europeo, non potrebbero trovare applicazione le rispettive leggi nazionali (e comunitarie).

Di contro, si registra un'impostazione alternativa volta a ribadire - in linea con la giurisprudenza non solo comunitaria ma anche (come si vedrà *infra*) Statunitense - che ciò che conta è il luogo dove il servizio *Web* viene offerto, anche ai fini dell'applicazione della relativa legge.

La questione, fra l'altro – come si accennava in precedenza – ha un'accentuata rilevanza pratica prima ancora che giuridica. Si pensi, ad esempio, al fenomeno Skype o, più in generale, a tutti i sistemi di comunicazioni Voice over IP (VoIP) criptati. Lo stato dell'arte, come si è detto *supra*, consente agli investigatori - in fatto ed in diritto - di disporre con successo una intercettazione solamente quando è noto il luogo esatto dove si trova il computer dell'indagato: solo così sarà possibile interagire con esso, installando un *trojan* o eventualmente – ove non sia possibile accedere fisicamente al luogo ove si trova il computer - utilizzando tecniche di *social enginering*[237] al fine di implementare un'intercettazione ex art.266 bis c.p.p. non soltanto sul canale comunicativo telematico (cioè a valle) bensì sulle comunicazioni originate da, ovvero in transito per, il computer in uso al soggetto bersaglio dell'operazione di monitoraggio (a monte, quindi).

4.3.d) segue: l'intercettazione di caselle di posta elettronica.

[237] Nel campo della sicurezza delle informazioni per ingegneria sociale (dall'inglese *social engineering*) si intende lo studio del comportamento individuale di una persona al fine di carpire informazioni.
Questa tecnica è anche un metodo (improprio) di crittanalisi quando è usata su una persona che conosce la chiave crittografica di un sistema e viene usata anche dalla polizia. Un ingegnere sociale (*social engineer*) per definirsi tale deve saper fingere, sapere ingannare gli altri, in una parola saper mentire. Un social *engineer* è molto bravo a nascondere la propria identità, fingendosi un'altra persona: in tal modo egli riesce a ricavare informazioni che non potrebbe mai ottenere con la sua identità reale. Il *social engineer* comincia con il raccogliere informazioni sulla vittima per poi arrivare all'attacco vero e proprio. Durante la prima fase (che può richiedere anche alcune settimane di analisi), l'ingegnere cercherà di ricavare tutte le informazioni di cui necessita sul suo bersaglio: e-mail, recapiti telefonici, ecc. Superata questa fase, detta *footprinting*, l'ingegnere passerà alla fase successiva, cioè quella che gli permetterà di verificare se le informazioni che ha ricavato sono più o meno attendibili, anche telefonando all'azienda del bersaglio e chiedendo cortesemente di parlare con la vittima. La fase più importante, quella che determinerà il successo dell'attacco, è lo studio dello stile vocale della persona per la quale vuole spacciarsi (ad esempio cercando di evitare in tutti i modi l'utilizzo di espressioni dialettali e cercando di essere quanto più naturale possibile, sempre utilizzando un tono neutro e cortese). Molto spesso il *social engineering* viene utilizzato per ricavare informazioni su privati (*phishing*). Un esempio di azione di questo genere può essere una falsa e-mail, mandata da un aspirante ingegnere sociale fingendosi magari un amministratore di sistema, o un membro di qualche grosso ente. Vengono richiesti al malcapitato di turno nome utente e *password* di un suo *account*, ad esempio quello di posta elettronica, con la scusa di fare dei controlli sul *database* dell'azienda. Se la vittima cade nel tranello, il social engineer avrà ottenuto il suo obiettivo, ossia una breccia nel sistema della vittima. Tecniche sofisticate di *"social engineering"* che fanno ampio uso di strumenti informatici e, segnatamente, delle reti, sono: il *crackeraggio*; il *phishing*; l'*hackeraggio;* il *lamerage*; lo *script kiddie*; la manipolazione; lo *scam*; il *social Network Poisoning*. Altre tecniche, meno sofisticate, ma ugualmente (empiricamente) sperimentate sono: rovistare nella spazzatura in cerca di foglietti con appuntate delle *password*, o comunque in cerca di recapiti telefonici indirizzi, ecc; fare conoscenza con la vittima, fingendo di essere un incompetente informatico e chiedendo lumi all'esperto; spacciarsi per un addetto della compagnia che vende i programmi utilizzati, dicendo che è necessario installare una *patch* al sistema.

E' noto come i più diffusi sistemi di posta elettronica siano offerti, a livello globale, da multinazionali americane. Le stesse, peraltro – per dire di ciò che accade non solo in Italia trattandosi, in realtà, di una questione dalla rilevanza mondiale - generano copiosi flussi di comunicazioni tra persone che, spesso, sono tutte presenti all'interno di un unico Stato diverso dagli Stati Uniti.

E' in questo ambito che si verifica, sempre più spesso, quanto già prima indicato in relazione alla teoria che potremmo definire del "*no server no law*".

È infatti noto agli addetti ai lavori come, rispetto alle società di telecomunicazione nazionali, sia possibile richiedere - in esecuzione del provvedimento del Giudice che dispone l'intercettazione telematica - che la posta elettronica indirizzata alla e-mail intercettata venga reindirizzata ad un *account* appositamente creato dalla Polizia Giudiziaria: questo consente non solo un risparmio dei costi delle complessive operazioni di intercettazione[238], ma anche soprattutto la possibilità di iniziarle in tempi ragionevolmente brevi (questione non di poco momento laddove sia addirittura in pericolo una vita umana).

Tuttavia, con riferimento a caselle di posta elettronica del tipo *"@.com"* questo meccanismo diventa spesso impossibile. infatti allorquando la Polizia Giudiziaria va a notificare ad esempio a Google o a Microsoft (entrambe aventi, quali filiali, una società di diritto italiano con sede in Milano) il decreto del Giudice che autorizza l'intercettazione, la tipica risposta che viene loro fornita suona più o meno in questi termini: *"Spiacenti, i nostri server stanno in America.... quindi chiedete l'intercettazione con una rogatoria!".*

Singolare è il caso di Yahoo (società Statunitense avente però, una filiale di diritto italiano, con sede pure a Milano). Essa dispone di un software *ad hoc* – denominato *"Yahoo Account Management Tool"* - che consente l'intercettazione delle caselle di posta elettronica (ma con alcuni limiti, il *tool* infatti è accessibile da molteplici soggetti all'interno delle varie filiali europee di Yahoo con potenziale pregiudizio, quindi, alla riservatezza degli utenti e, di conseguenza, anche per le stesse indagini di polizia giudiziaria).

Ora, è interessante notare come sulla base del principio della "*Net Citinzenship"* (cittadinanza di rete), l'utente può scegliere (anche inconsapevolmente) - al momento della registrazione di una *e-mail "@yahoo"* – a quale legislazione sottoporre la sua casella di posta elettronica e solamente ove abbia scelto quella italiana (*yahoo.it*, anziché *yahoo.com*), il richiamato *software* ne consentirà l'intercettazione immediata ove necessaria ai fini investigativi ed autorizzata con provvedimento dell'Autorità Giudiziaria.

Analoghe considerazioni valgono relativamente ai dati prodotti dal traffico telematico e più precisamente rispetto all'ordine di esibizione dei *c.d. file di log* (su cui si veda il para 4.1.f) *supra*).

[238] Diversamente, occorrerebbe dapprima richiedere i tabulati telefonici del numero utilizzato per la connessione ad Internet (per verificare quale sia il gestore che la fornisce) e successivamente pianificare, d'intesa con il gestore, l'azione di collocamento delle c.d. sonde (tecnicamente necessarie per intercettare il traffico utile): nel complesso tali operazioni possono durare anche una intera settimana!

Nonostante la tendenza attuale sia nel senso della massima collaborazione possibile degli ISP (soprattutto da parte dei colossi americani delle comunicazioni) con le Autorità inquirenti dei diversi Stati, si continua tuttavia, ancor oggi, a registrare una *policy* di difficile comprensione circa il fondamento giuridico in virtù della quale vengono forniti i dati richiesti dalle Autorità solamente laddove l'IP interessato rientri nel *range* assegnato a Paesi Membri UE (diversamente, viene indicato la sola localizzazione dell'IP richiesto corredata dalla annotazione circa l'impossibilità di comunicare i relativi dati ad Autorità Giudiziarie diverse da quelle dello Stato interessato).

4.3.e) segue: *"Law Enforcement requests".* Policy di Microsoft[239].

Emerge un quadro sufficientemente articolato nel è possibile individuare numerose ed articolate questioni di ordine giuridico. Partendo infatti da una generica *notitia criminis* (raccolta dalle Autorità preposte alla persecuzione dei reati) connotata (in qualche modo) dalla presenza - per così dire - di elementi cibernetici, ci si sposta inesorabilmente su altri complessi ambiti del diritto. Si va infatti dalla tutela e dalla garanzia, sovente di rango Costituzionale, delle comunicazioni tra soggetti fino ad arrivare alla disciplina concernente il rispetto della riservatezza della sfera personale degli individui, passando peraltro attraverso la disciplina che regola le c.d. prestazioni obbligatorie (o di giustizia) cui sono tenute le società che gestiscono i servizi di comunicazione elettronica e la connessa regolamentazione giuridica della materia cosiddetta dei *"data retention"*. Tutto, fra l'altro, è reso ancor più complicato dal fatto di stagliarsi in una dimensione internazionalistica nella quale si distinguono soggetti (per l'appunto le grandi Corporation americane) che agiscono in più contesti nazionali pur senza possedere sedi legali e/o filiali in tutti i Paesi nei quali svolgono il proprio *busisness*.

Da qui la necessità per dette industrie dell'informatica e delle comunicazioni di stabilire, nel rispetto comparativistico dei diversi ordinamenti in cui si trovano ad operare, rapporti precisi di collaborazione con le autorità dei singoli Stati senza sacrificare, al contempo, il necessario rapporto fiduciario intercorrente con i propri clienti/utenti. Rapporto che non può che basarsi sulla gestione trasparente e scrupolosa dei dati e delle informazioni (quasi sempre a carattere riservato) riguardanti i fruitori dei propri servizi. Ma che al tempo stesso non può prescindere dal doveroso rispetto delle norme positive vigenti nei singoli Stati. Ed è proprio in ossequio al predetto principio di trasparenza e di minor pregiudizio possibile che le più importanti società del settore rendono palese ai propri consumatori le *policy* e le procedure mediante le quali, dando ottemperanza (ove ve ne siano) ai propri obblighi, cercano di contemperare ogni contrapposta pretesa.

---

[239] Le informazioni riportate in questo paragrafo sono tratte dal "*Microsoft - 2012 Law Enforcement Requests. Report. Principles, Policies and Practices".*

Per quanto concerne in particolare Microsoft (cui fanno capo Skype, Hotmail, Outlook, Messanger ecc. ecc.), la società sottolinea che in linea di principio vengono considerate, esclusivamente, le richieste delle Autorità inquirenti (di solo quarantasei Paesi) che si rendono rispettose delle norme e delle procedure, formali e sostanziali, vigenti nei singoli Stati, con l'ulteriore precisazione che il paradigma, per ciò che riguarda le richieste che attengono dati dei propri clienti a contenuto c.d. "non comunicativo" (o dati esterni, quali informazioni di base sul conto dell'utente, storico delle connessioni IP ecc.), è rappresentato da un valido *subpoena*[240], laddove richieste aventi ad oggetto dati dei propri utenti a "contenuto comunicativo" debbono, per poter essere processate, promanare direttamente da un "ordine giudiziale".

E ancora, le richieste (formate nel senso detto sopra) debbono essere inviate rispettivamente agli uffici Irlandesi o Californiani a seconda se riguardano *account* Microsoft creati in Europa o nel resto del Mondo, laddove tutte le richieste riguardanti Skype debbono essere indirizzate agli uffici del Lussemburgo.

Le istanze formulate in una lingua diversa dall'inglese, se indirizzate a Microsoft, vengono tradotte ed autenticate (con l'indicazione della corrispondenza alle leggi ed alle procedure vigenti nel Paese proponente) da un avvocato di Microsoft (operante nel paese di origine della domanda) che ne curerà la trasmissione agli uffici competenti (Irlandesi o Americani). Laddove le richieste rivolte a Skype possono essere redatte nella stessa lingua ufficiale dello Stato da cui promanano venendo tradotte direttamente nel Lussemburgo.

Per quanto concerne poi le norme giuridiche applicabili, Microsoft evidenzia che i dati ospitati nei server americani (a prescindere dal paese di autenticazione del cliente) vengono rilasciati alle Autorità richiedenti alla stregua dell'"*Electronic Communications Privacy Act",* mentre i dati di Outlook od Hotmail immagazzinati nei server europei vengono trattati alla stregua delle leggi irlandesi e delle direttive europee.

Le richieste rivolte a Skype, invece, soggiacciono alle norme del Lussemburgo. Ciò non toglie che non si possa dare seguito alle istanze provenienti da altri paesi (lo si è detto poc'anzi), ma soltanto che i dati verranno rilasciati alla stregua delle leggi Statunitensi, Irlandesi (e pertinenti direttive europee) e Lussemburghesi. Rimanendo pertanto le Autorità dei predetti tre Paesi quelle alle quali Microsoft si impegna, per certo, a dare immediatamente e prontamente seguito ad ogni eventuale richiesta validamente (da un punto di vista procedurale) avanzata.

Microsoft sottolinea inoltre che, a prescindere da qualsivoglia richiesta in tal senso - e quindi anche di propria iniziativa - provvederà a rilasciare i dati opportuni alle competenti Autorità tutte le volte in cui si ritroverà ad essere parte offesa di un

[240] In termini estremamente generici, un *subpoena* è nel diritto di tipo anglosassone un invito rivolto per via giudiziale da una parte processuale (e quindi anche dall'accusa) ad un soggetto terzo (estraneo quindi ai fatti per i quali si procede) di presentarsi per rendere una testimonianza ovvero di fornire, entro un certo termine, determinata documentazione in suo possesso.

delitto ovvero, in applicazione di speciali norme, laddove si imbatterà in reati in materia di pornografia minorile.
Vengono, infine forniti, per maggior completezza, i dati relativi alle richieste giudiziali pervenute nell'anno 2012, indicate complessivamente in 137.000 unità circa, pari cioè allo 0.02% del totale degli utenti registrati sui servizi riconducibili a Microsoft.

4.3.f) segue: *"Law Enforcement requests".* I "*Mutual Legal Assistance Treaty",* l'*Electronic Communications Privacy Act* e la Policy di Google[241].

È interessante notare, innanzitutto, ciò che Google asserisce in ordine alle richieste, per fini di indagini penali, che promanano da Stati "non solitamente avvezzi" ad inoltrare istanze di collaborazione alla società californiana (ai fini di intercettazione o altro). Quando cioè esse risultano di numero assai limitato (meno di 30 in un anno), Google afferma di non includere dette richieste in alcuna statistica ufficiale e ciò al solo scopo di impedire che la *"…divulgazione delle statistiche possa mettere a rischio importanti indagini e possa interferire con le iniziative a tutela della sicurezza pubblica messe in atto delle autorità competenti".*
Anche Google sottolinea che ogni richiesta viene sottoposta ad un accurato vaglio di legalità sia formale sia sostanziale e che non tutte, anche se promananti dalle autorità competenti, vengono accolte.
Per quanto concerne le *National Security Letters*[242] (NSL), gli unici dati che Google è tenuta a fornire all'FBI, ai sensi dell'*Electronic Communications Privacy Act* (ECPA)[243], sono: nome, indirizzo, anzianità di registrazione ad un servizio, certificazioni relative ai pagamenti, dati di abbonamento, raggio del "pedaggio" (a breve e/o lunga distanza) relativi ad un abbonato a servizi di comunicazione via cavo o elettronica. L'FBI peraltro non può ricorrere alle NSL per ottenere da Google informazioni di altro tipo, quali "contenuti" Gmail, query di ricerca, video di YouTube visualizzati o caricati

---

[241] Le informazioni riportate in questo paragrafo sono, per buona parte, tratte dalla sezione "privacy" del sito istituzionale *Google.com*

[242] Si tratta di una richiesta di informazioni che può essere presentata dall'FBI (Federal Bureau of Investigation) o da altre agenzie del ramo investigativo del governo degli Stati Uniti in caso di indagini per la sicurezza nazionale. Non è possibile ricorrere alle NSL per questioni penali, civili o amministrative ordinarie. L'FBI è tenuta a riferire al Congresso il tipo di ricorso alle NSL ogni sei mesi. Anche il Dipartimento di Giustizia degli Stati Uniti effettua controlli regolari sulla modalità di utilizzo delle NSL da parte dell'FBI. Il direttore dell'FBI od un funzionario "senior" designato è tenuto a fornire una certificazione scritta che dimostri che le informazioni richieste siano "pertinenti a un'indagine autorizzata per la tutela da azioni di terrorismo internazionale o di spionaggio illegale". L'FBI non è tenuta a ottenere l'approvazione di un tribunale per poter emettere una NSL.
Come avviene del resto per le intercettazioni, anche rispetto alle NSL è prassi di Google informare gli utenti in caso di richieste legali, se opportuno e se non è vietato dalla legge o da un'ingiunzione di un tribunale. L'FBI peraltro ha il potere di vietare al destinatario di una NSL di divulgare il fatto di avere ricevuto tale NSL certificando che la divulgazione potrebbe comportare un rischio per la sicurezza nazionale degli Stati Uniti, interferire con un'indagine penale in materia di antiterrorismo o di controspionaggio, interferire con i rapporti diplomatici o più semplicemente mettere in pericolo la vita o la sicurezza fisica di una persona.

[243] Su cui cfr. *infra.*

in rete dagli utenti, indirizzi IP dei medesimi, oggetto e destinazione delle mail (per tutte queste saranno necessarie le c.d. "perquisizioni" o "ingiunzioni" su cui *infra*)
Le NSL non sono peraltro una prerogativa esclusiva degli Stati Uniti e Google si dichiara pronta a dare ottemperanza agli analoghi provvedimenti delle Autorità governative di altri Stati purché siano rispettosi delle norme e delle procedure legali vigenti nei medesimi Stati.
Per quanto concerne appunto le richieste provenienti da Autorità (governative e/o giudiziarie) di Paesi diversi dagli U.S.A., le stesse, secondo quanto indicato da Google, debbono seguire, per poter trovare accoglimento, il canale dei *Mutual Legal Assistance Treaty* (MLAT). Un MLAT è sostanzialmente un trattato tra gli Stati Uniti e un altro Paese che definisce le procedure (per lo più rogatorie od altre procedure semplificate) attraverso le quali tali Paesi si aiuteranno a vicenda nelle questioni legali, ad esempio nelle indagini penali. Attraverso un MLAT, un governo straniero potrà chiedere pertanto al governo degli Stati Uniti aiuto nella raccolta di prove presso entità statunitensi, incluse società come Google. Se il governo degli Stati Uniti approverà la richiesta, Google risponderà e presterà la sua collaborazione esattamente negli stessi termini qualora la richiesta provenisse direttamente dalle Autorità Statunitensi.

Ora, è appena il caso di ricordare come gli Stati Uniti già da diversi anni abbiano ratificato la Convenzione di Budapest sul *cybercrime*. Detta Convenzione - alla quale fra l'altro aderiscono quasi tutti i Paesi della U.E. - detta come noto norme specifiche, per lo più con finalità di semplificazione, in materia di mutua assistenza giudiziaria fra i Paesi aderenti.
Più precisamente, costituiscono oggetto dell'assistenza giudiziaria tutte le attività d'indagine che la Convenzione individua come "tipicamente" necessarie a combattere il crimine informatico: si allude perciò alla perquisizione, all'accesso a sistemi informatici situati all'estero, al loro sequestro, alla conservazione in tempo reale dei dati relativi al traffico ed infine, ovviamente, alle intercettazioni del contenuto di comunicazioni trasmesse attraverso l'uso di sistemi informatici (artt. 31, 33 e 34 della Convenzione di Budapest).
È opportuno peraltro segnalare due novità di assoluto rilievo introdotte dalla Convenzione nella predisposizione degli strumenti di assistenza.
La prima (art. 29) riguarda la possibilità che una Parte, ancor prima di inoltrare una commissione rogatoria, possa richiedere ed ottenere da un'altra Parte la misura provvisoria della conservazione rapida di dati informatici immagazzinati attraverso un sistema informatico situato all'estero. La conservazione dei citati dati dovrà essere curata dalle Autorità della parte richiesta per un tempo non inferiore a sessanta giorni, in attesa che la Parte richiedente formalizzi una richiesta di mutua assistenza per la perquisizione, l'accesso ad un sistema informatico, ovvero per il sequestro dei dati oggetto di ricerca. Si tratta di disposizione che riveste grande utilità nelle indagini informatiche su scala internazionale e che conferisce a quest'ultime quella snellezza e quella celerità, indispensabili per contrastare efficacemente l'estrema "volatilità"

delle tracce dei reati in danno di sistemi informatici, ovvero commessi con l'uso dei medesimi sistemi.
Altra disposizione di forte contenuto innovativo (art. 32) è quella che disciplina l'accesso transfontaliero a dati immagazzinati in sistemi informatici situati all'estero. Si tratta dell' "adattamento" alle investigazioni *in subiecta materia* di uno strumento già introdotto dal Protocollo di adesione all'Accordo di Schengen (art. 41 della L. 388/1993, che prevede appunto l'inseguimento transfrontaliero – senza necessità di previa autorizzazione delle Autorità della Parte contraente nel cui territorio si debba continuare l'inseguimento - di una persona colta in flagranza di reato per taluni gravi delitti specificati al 4° comma del medesimo articolo).
La Convenzione di Budapest consente infatti l'accesso "virtuale" delle Autorità di una Parte (i.e. Stato), senza necessità di autorizzazione dell'altra Parte (i.e. Stato), ai dati informatici immagazzinati e disponibili al pubblico, senza aver riguardo al luogo geografico in cui si trovano tali dati; e consente anche l'accesso altrettanto "virtuale" - a mezzo di un sistema informatico collocato sul proprio territorio - a dati informatici (ovvero la loro ricezione) situati in un altro Stato, sempre che vi sia il consenso "legale e volontario" di chi ha l'autorità legale di divulgare i medesimi dati (vale a dire i *providers*).
Ciò comporta pertanto – sottolinea Google – la possibilità che la Società ottemperi, *sua sponte,* a richieste di informazioni di emergenza provenienti da Autorità straniere quando ciò possa prevenire lesioni fisiche gravi o letali per qualcuno.
Google si dichiara infatti disponibile a fornire, volontariamente, dati relativi ai propri utenti in risposta a un procedimento legale esperito da enti statali non statunitensi, a condizione che tali richieste siano conformi alle normative internazionali, al diritto statunitense, alle norme di Google e alle leggi del Paese richiedente.
Cionondimeno, le procedure legali vigenti negli Stati Uniti - in virtù delle quali le società che operano nel settore ICT *(information and communication technology)* sono tenute a divulgare in via riservata alle Autorità inquirenti i dati di cui sono in possesso relativi ai propri utenti – sono contemplate in una legge federale denominata *Electronic Communications Privacy Act* (ECPA). Dette procedure sono essenzialmente riconducibili a tre differenti tipologie di atti: le *citazioni*, le ingiunzioni e le perquisizioni.

Dei tre tipi di procedimenti legali previsti dall'ECPA, *la citazione* è quella più facile da ottenere per un ente statale. In molte giurisdizioni, compreso il sistema federale, non è assolutamente necessario che un giudice o un magistrato esamini una citazione prima che il governo la possa emettere. Tuttavia, l'ente statale può ricorrere ad una citazione esclusivamente per ottenere limitate informazioni. Ad esempio il nome associato ad un *account,* ovvero gli indirizzi IP da cui l'account stesso è stato creato, quando è stato eseguito l'accesso ed effettuata la disconnessione dell'utente (con date e orari) ed in pochi altri limitati casi. Le citazioni peraltro possono essere utilizzate sia per casi civili sia per questioni penali.
Per ottenere un'*ingiunzione* è invece necessario un previo controllo giurisdizionale. L'Autorità inquirente deve infatti dimostrare l'esistenza di motivi ragionevoli che

inducono a ritenere che la prova di un reato non potrà rinvenirsi se non nelle informazioni richieste.
Con tale ingiunzione del tribunale, un ente statale può ottenere le stesse informazioni che è possibile ottenere con una citazione, oltre a informazioni più dettagliate sull'utilizzo dell'account. Tali informazioni possono includere l'indirizzo IP associato a una determinata email inviata dall'*account* o utilizzata per cambiare la *password* dell'*account* (con date e orari), nonché la parte relativa alle intestazioni delle email (quali i campi "da", "a" , "oggetto" e "data" (ma non i contenuti di quella e-mail). Un'ingiunzione del tribunale inoltre è disponibile soltanto per indagini penali.
Ottenere un mandato di *perquisizione ECPA* è ancora più difficile. Per ottenerne uno, infatti, l'Autorità statale deve presentare la richiesta a un giudice o magistrato e soddisfare un onere della prova relativamente alto: dimostrare cioè la necessità di ricercare, con tempestività, determinate informazioni relative a un reato in un luogo specifico. Il mandato deve pertanto indicare il luogo da perquisire e gli elementi cercati. Può essere utilizzato per imporre la divulgazione delle stesse informazioni di una citazione o un'ingiunzione del tribunale ECPA, ma anche di informazioni sulle *query* di ricerca di un utente e di contenuti privati memorizzati in un account Google, come messaggi Gmail, documenti, foto e video di YouTube. Il mandato di perquisizione ECPA è disponibile soltanto per indagini penali[244].

[244] Ecco alcuni esempi dei tipi di dati che Google può essere costretta a divulgare, a seconda del procedimento legale ECPA esperito, dell'entità della richiesta e di ciò che è richiesto e disponibile:

Gmail

Citazione:

- Informazioni di registrazione dell'iscritto (ad es. nome, informazioni sulla creazione dell'account, indirizzi email associati, numero di telefono)
- Indirizzi IP di accesso e time-stamp associati

Ingiunzione del tribunale:

- Informazioni non relative ai contenuti (come informazioni sulle intestazioni delle email)
- Informazioni ottenibili con una citazione

Mandato di perquisizione:

- Contenuti e-mail
- Informazioni ottenibili con una citazione o un'ingiunzione del tribunale

YouTube

Citazione:

- Informazioni di registrazione dell'iscritto
- Indirizzo IP di registrazione e time-stamp associati

4.3.g) Gli obblighi di mutua assistenza con gli U.S.A. derivanti dalla *Convenzione sul Cybercrime*.

Ingiunzione del tribunale:

- Indirizzo IP di caricamento video e time-stamp associato
- Informazioni ottenibili con una citazione

Mandato di perquisizione:

- Copia di un video privato e informazioni video associate
- Contenuti di messaggi privati
- Informazioni ottenibili con una citazione o un'ingiunzione del tribunale

Google Voice

Citazione:

- Informazioni di registrazione dell'utente
- Indirizzo IP di registrazione e time-stamp associato
- Registrazioni di connessione telefonica
- Dati di fatturazione

Ingiunzione del tribunale:

- Numero di deviazione
- Informazioni ottenibili con una citazione

Mandato di perquisizione:

- Contenuti degli SMS memorizzati
- Contenuti della segreteria memorizzati
- Informazioni ottenibili con una citazione o un'ingiunzione del tribunale

Blogger

Citazione:

- Pagina di registrazione del blog
- Informazioni di iscrizione del proprietario del blog

Ingiunzione del tribunale:

- Indirizzo IP e time-stamp associato relativi a un post specifico sul blog
- Indirizzo IP e time-stamp associato relativi a un commento specifico su un post
- Informazioni ottenibili con una citazione

Mandato di perquisizione:

- Contenuti di post e commenti privati del blog.

Per quanto concerne poi il complessivo sistema delle intercettazioni, la legislazione americana, in ossequio a precisi limiti costituzionali, impone precisi divieti in relazione alla possibile captazione e trasmissione del contenuto di comunicazioni a soggetti terzi, in assenza di un provvedimento *ad hoc* promanante dalla competente (anche territorialmente) Autorità Giudiziaria. La *ratio* di tale previsione è di agevole comprensione: si tratta di garantire i fondamentali diritti degli utenti e di sottoporre le richieste aventi ad oggetto la limitazione di un diritto costituzionalmente garantito al vaglio dell'Autorità Giudiziaria che abbia effettiva giurisdizione in relazione al territorio ove si svolgono i fatti (e ove, verosimilmente, abbiano cittadinanza le persone che di tali fatti sono i protagonisti). E dunque, tradizionalmente, all'Autorità Giudiziaria statunitense.

Ma il mondo è cambiato rapidamente e una situazione di fatto impensabile fino a 15 - 20 anni fa è adesso diffusamente all'ordine del giorno: ovvero che persone non fisicamente presenti sul territorio di uno Stato possano utilizzare sistemi di comunicazione viceversa fisicamente localizzati in quello Stato. E, ancor di più, che tali persone non abbiamo neppure cittadinanza in quello Stato!

E proprio per questo si impone, nello specifico tema oggetto della nostra analisi, una riflessione in punto di giurisdizione: nello specifico, laddove il Giudice italiano attesti (come peraltro avviene anche oggi) che tali sistemi di comunicazione (fisicamente allocati negli Stati Uniti, quantomeno in relazione ai *server* interessati) siano utilizzati, da remoto, da cittadini italiani, quali ulteriori ostacoli normativi residuerebbero?

Non potrebbe cioè lo Stato italiano nella sua componente di Giustizia, al verificarsi di casi consimili, affermare, ragionevolmente, la propria giurisdizione in materia, essendo solo un accidente (o se del caso un agevole espediente di *forum shopping*) quello relativo alla diversa localizzazione di un servizio di comunicazione utilizzato peraltro da propri cittadini integralmente ed esclusivamente sul territorio italiano?

Si è visto, nel precedente paragrafo, come alla base dei vincoli e degli obblighi di collaborazione in capo ai gestori dei più svariati servizi di comunicazione, si pongano spesso, quale unico rimedio esperibile, soltanto gli strumenti offerti da specifici trattati di mutua assistenza legale, gli unici a garantire alle Autorità di un altro paese la possibilità di ottenere da società ed operatori americani risposte complete ed esaustive alle proprie istanze al pari di quelle che riceverebbero le competenti Autorità Statunitensi qualora attivassero le relative procedure di diritto domestico.

Ebbene, gli Stati Uniti già da tempo hanno ratificato la Convenzione di Budapest che prevede - proprio nelle materie oggetto di trattazione - due precisi obblighi di collaborazione *"in tempo reale"* (art. 33 in materia di raccolta dei dati del traffico; art. 34 in materia di intercettazione dei contenuti)[245]. E dunque, dal momento che anche

[245] *Art.33 Convenzione di Budapest:*

Mutua assistenza nella raccolta in tempo reali di dati di traffico.

1. Le parti devono fornire mutua assistenza tra loro nella raccolta in tempo reale di dati sul traffico, associati a specifiche comunicazioni nel proprio territorio, trasmessi attraverso l'uso di un sistema informatico. Questa assistenza, soggetta alle disposizioni del paragrafo 2, è regolata dalle condizioni e dalle procedure previste dal diritto interno.

l'Italia ha ratificato detta Convenzione, tali obblighi oggi acquistano una loro considerevole portata oltre che un'effettiva valenza giuridica (bilaterale), in ossequio al principio generale di diritto internazionale secondo cui *pacta servanda sunt*[246].
In particolare, laddove le predette società di diritto americano, con atteggiamento refrattario o non del tutto collaborativo, continuassero a considerarsi completamente estranee e, pertanto, non soggette alle normative europee, le Autorità Giudiziarie nazionali potrebbero sensatamente agire in maniera del tutto fondata e giuridicamente corretta[247] non solo nei confronti delle locali Autorità amministrative competenti[248], ma anche, a ben vedere, nei confronti di quelle americane, al legittimo fine di ottenere una celere e corretta applicazione della più volte citata Convenzione di Budapest.

4.4. Le intercettazioni telematiche ed informatiche.

4.4.a) Modalità tecniche ed esperienziali di esecuzione delle intercettazioni telematiche ed informatiche.

La premessa fondamentale dalla quale prendere le mosse è che le attività intercettive, per poter condurre a risultati remunerativi, dovranno sempre necessariamente focalizzarsi su quei punti e canali di comunicazione che le esperienze e le tecnologie degli ultimi anni hanno permesso di accertare ed identificare come "canali sensibili". E quindi, molto sinteticamente, concentrarsi su linee ADSL, *dongle* USB (c.d. penne usb), connessioni *wireless*, *email*, *chat*, *forum*, *social network* ecc. ecc. . Deve precisarsi altresì che, a prescindere dall'effettuazione

---

2.Tutte le parti devono fornire questa assistenza almeno rispetto ai reati per i quali la raccolta in tempo reale dei dati sul traffico sarebbe possibile, in ambito interno, in una situazione analoga.
Art. 34 Convenzione di Budapest:
Mutua assistenza in materia di intercettazione di dati relativa al contenuto.
Le parti devono fornirsi mutua assistenza nella raccolta o registrazione in tempo reale di dati relativi al contenuto di specificate comunicazioni trasmesse attraverso l'uso di un sistema informatico nella misura consentita dai trattati applicabili fra le stesse e dalle leggi interne.

[246] Maggiori spunti di riflessione saranno offerti dal para. 4.5.b), *infra.*

[247] Si pensi alla condanna di 55.000 euro, oltre a 10.000 curo per ogni giorno successivo di inadempimento, inflitta dal Tribunale belga di Den- dermonde a Yahoo! Inc. (che peraltro non ha neppure una filiale in Belgio) per non aver fornito informazioni sul titolare di una casella di posta elettronica. Cfr. in Internet: http://www.techcrunch.com/2009/03/02/yahoo-fined-by-belgian-court-for-refusing-togive-up-e-mail-account-info .

[248] Quanto alla situazione italiana, l'art. 5 comma 2 d.lvo 109/08 così prevede: *«Salvo che il fatto costituisca reato, l'omessa o l'incompleta conservazione dei dati ai sensi dell'articolo 132, commi 1 e 1-bis, del Codice, è punita con la sanzione amministrativa pecuniaria da euro 10.000 ad euro 50.000 che può essere aumentata fino al triplo in ragione delle condizioni economiche dei responsabili della violazione. Nel caso di assegnazione di indirizzo IP che non consente l'identificazione univoca dell'utente o abbonato si applica la sanzione amministrativa pecuniaria da 5.000 euro a 50.000 euro, che può essere aumentata fino al triplo in ragione delle condizioni economiche dei responsabili della violazione. Le violazioni sono contestate e le sanzioni sono applicate dal Ministero dello sviluppo economico».*

di specifiche intercettazioni, le conoscenze maturate sul campo hanno da tempo permesso alla Polizia Giudiziaria di accertare ed identificare molteplici vulnerabilità dei vari protocolli comunicativi utilizzati dai criminali informatici che escludono l'effettuazione di intercettazioni *stricto sensu*. Queste vulnerabilità, va detto, potranno in molti casi assumere esclusivamente la veste di mere fonti informative; ciò non toglie tuttavia che, ove possibile, il loro proficuo sfruttamento deve poter condurre all'acquisizione di dati ed informazioni producibili (*rectius* "riproducibili")in forma intellegibile in fase dibattimentale.

Per quanto concerne poi nello specifico le concrete modalità operative di esecuzione delle intercettazioni telematiche ed informatiche, queste sono fortemente condizionate dalle distinte caratteristiche del sistema oggetto delle attività di captazione, nonché dal tipo di informazioni ("flussi di comunicazioni", per lo più a carattere digitale) che si intendono acquisire.

Occorre perciò in primo luogo accertare il tipo di *"protocollo"* utilizzato per la trasmissione dei dati che si vogliono intercettare. Esistono infatti diversi servizi che si possono intercettare e la loro intercettazione può corrispondere ad azioni legali di natura differente. L'intercettazione delle *email*, per esempio, che avviene di regola deviando su un'apposita casella clone tutto quello che riceve o invia un soggetto, concerne come è evidente la materia della captazione di corrispondenza. Si possono poi intercettare i movimenti dati su un sito *web* (*uploading* & *downloading*), le comunicazioni tramite *chat*, in linea di principio il *VoIP*, ecc. ecc..

Nella maggioranza dei casi il gestore dei servizi di comunicazione, definita un'apposita "griglia" di selezione delle comunicazioni, fornirà alla polizia giudiziaria una linea telefonica, definita linea RES, dedicata allo sviluppo dell'attività di intercettazione. Tale linea può essere presa a noleggio da parte della procura presso il gestore, oppure presso società private o consorzi. Ad ogni modo, la linea RES viene attestata presso la sala intercettazioni della procura, dove vi è un *server* presso il quale viene convogliato il traffico telefonico e/o dati delle utenze di cui l'AG ha disposto il controllo.

Ogni volta inoltre che l'utente si collega ad un *Internet Service Provider* (ISP) per avere la connessione alla rete Internet ottiene, come più volte detto *supra*, uno specifico indirizzo IP: prima dell'attribuzione dell'indirizzo, l'utente viene identificato *(*in gergo *"logato")* dal *server* come soggetto abilitato a ricevere i propri servizi, previo riconoscimento degli estremi identificativi del *client* (*username* e *password*) ed in tal modo accettato ed abilitato alla navigazione in Internet.

Una volta riconosciuto dal sistema, all'utente viene assegnato un numero IP dinamico (nel senso che sarà diverso alla prossima connessione) che seguirà la sua navigazione, e che identificherà univocamente la sua macchina durante tutta la durata di quel "collegamento".

Inoltre, per poter accedere ai servizi offerti da un *server*, ogni *client* deve poter identificare il servizio con precisione, così da inviare una richiesta univoca. I servizi richiesti ai *servers* sono abbinati ai cd. *port numbers*, numeri cioè che caratterizzano ogni specifica funzionalità disponibile su un *server* attivo su un elaboratore: proprio

attraverso l'indicazione del *"port number"*, i singoli utenti della rete possono avere accesso alle varie applicazioni disponibili sul *server* al quale è stata inviata la richiesta. I canali di comunicazione riguardanti dati digitali possono peraltro essere di natura variegata: telefonia fissa (PSTN), mobile (GSM, GPRS, UMTS,ecc.), su Internet (VoIP), servizi Internet su banda larga, telefonia satellitare, ecc.. Data poi l'ampiezza di banda mediamente disponibile sugli attuali canali di comunicazione - fattore che promette continua crescita negli anni - la quantità di dati trasportata è immensa e richiede sicuramente l'esperimento di due attività preliminari: il "filtraggio" (esclusione della maggioranza dei dati che ai fini delle indagini risultano generalmente inutile) e la "correlazione" (non solo bisogna individuare le poche informazioni veramente utili, ma spesso senza correlarle il risultato è nullo). A questo va aggiunta la necessità di operare in tempi strettissimi in quanto ampiezza di banda significa anche minimi tempi di trasmissione e quindi difficoltà di rilevazione.

Ora, calandoci nello specifico, l'intercettazione telematica si articola su taluni caratteristici (e ricorrenti) passaggi tecnici. Occorre infatti:

- decriptare un segnale digitale e memorizzarlo su un apposito supporto;
- ma, ancor prima, individuare il *client* cui riferire la comunicazione, e poi individuare il soggetto *(persona fisica)* che abbia avuto in uso la macchina e che abbia effettuato la connessione durante la quale è stato consumato l'illecito. Di certo - stante il principio della responsabilità personale - non ci si potrà accontentare di identificare il numero di telefono chiamante o chiamato, ma occorrerà approfondire le indagini con accertamenti documentali (contratti, moduli di fatturazione,ecc.) ovvero storici (analisi delle ulteriori chiamate effettuate) nel tentativo di appurare la concreta disponibilità dell'utenza e della macchina ad un soggetto fisico ben individuato.

L'analisi dei dati intercettati, poi, si articola tipicamente secondo il seguente modulo:

a) ogni *server* di accesso alla rete, come ripetutamente detto *supra*, al momento della connessione (*"log-in"*) crea un *file* di *log* dell'utente, contenente le seguenti informazioni-base:

- *user name*;

- data, ora e secondi dell'inizio della connessione (*log-in*) e del termine della connessione (*logo-ut*);

- IP dinamico assegnato e *caller ID*, cioè numero del telefono chiamante;

b) qualora l'utente si colleghi ad un *server* di posta elettronica (un *server* cioè di 2° livello, differente dal server fornitore di connettività – c.d. *provider*), esso annoterà a sua volta l'accesso, registrando ancora:

- *user name;*

- data, ora e secondi del *login* e del *logout* sincronizzati su *"time server"*[249]*;*

- IP dinamico;

Ma non soltanto. Parametri altrettanto oggettivi quali le coordinate geografiche, i c.d. *Mac Address*[250] , le interfacce di rete *wireless* degli *Access Point* (difficilmente modificabili), possono essere presi in considerazione al fini di accertare in dibattimento il dipanarsi di operazioni tanto volatili come il monitoraggio delle reti *wireless* in un dato punto geografico.
Sulla base degli elementi sopra indicati sarà quindi possibile (cercare di) risalire all'effettivo utilizzatore delle linee telefoniche utilizzate per la connessione (caller ID chiamanti) e quindi ai singoli utenti, incrociando le informazioni derivanti dai dati costituiti dai *file* di *log*, dai dati di registrazione presso il *provider*, da quelli risultanti dal tabulato telefonico dell'utenza dalla quale risulta effettuato il collegamento al provider nonché dagli altri ulteriori parametri di cui si è detto.
In quest'ottica, peraltro, le problematiche con le quali ci si deve misurare sono quelle connesse all'impiego di Internet in combinazione con i vari servizi di anonimizzazione esistenti (proxy, anonymizer a pagamento, algoritmi di crittazione ecc. ecc.), all'impiego di SIM o USIM estere o rubate/trafugate, ovvero con la possibilità di sfruttare la connettività offerta da c.d. "Internet Cafè" non pienamente adempienti delle normative vigenti. Accorgimenti cioè che consentono ad operatori (anche non molto esperti) di assicurarsi un notevole livello di anonimato.
Come si accennava *supra*, dal punto di vista tecnico, la captazione dei flussi sottoposti ad intercettazione può essere effettuata: *deviando* i medesimi flussi sul *sistema intercettante*, che provvederà a memorizzarli e, quindi, a ritrasmetterli al destinatario; ovvero inserendo sul computer intercettato un "registro degli eventi" in grado di memorizzare gli inserimenti dei dati di interesse investigativo; oppure ancora - nel caso di intercettazioni telematiche - registrando i flussi dopo aver provveduto ad attivare un'apposita linea telefonica (RES,cfr. *supra*) fornita di modem per ricevere le comunicazioni oggetto delle indagini.
Le operazioni di intercettazione potranno inoltre avvenire o direttamente sulla linea telefonica dell'utente, interponendosi tra utente e provider, ovvero sfruttando la stessa rete del *provider*.
In atto le tecnologie d'intercettazione più diffuse sono costituite dagli analizzatori di protocollo. Di *protocol analyzer* se ne trovano numerosi disponibili gratuitamente (*open source*) anche sul *web*. Essi sono installati presso i *provider* e sono in grado di intercettare tutto il flusso dati relativo ad una determinata linea di comunicazione. Su

---

[249] Computer presenti nella rete Internet il cui compito consiste nel sincronizzare gli orologi dei computer all'interno di una rete di commutazione di pacchetto (Intenet) utilizzando il protocollo NTP :Il **Network Time Protocol**.

[250] In informatica e telecomunicazioni l'indirizzo MAC (in inglese MAC *address*, dove MAC sta per *Media Access Control*), detto anche indirizzo fisico, indirizzo *ethernet* o indirizzo LAN, è un codice di 48 bit (6 byte) assegnato in modo univoco dal produttore ad ogni scheda di rete ethernet prodotta al mondo (peraltro esistono software in grado di camuffare detto codice).

tale flusso dati si possono anche impostare taluni filtri al fine di selezionare i dati da catturare in ragione di specifiche esigenze investigative.

L'utente di un servizio internet, come noto, vi può accedere da diversi punti e con diverse tipologie di collegamento. Se è palese che il soggetto cambia continuamente via di collegamento, magari perché in movimento o perché avveduto della possibilità di essere controllato, bisogna impiegare una metodologia di intercettazione che operi contemporaneamente su più canali (audio/video/dati). A tal fine, frequentemente impiegato nelle indagini informatiche è il cd. "telemonitor": si tratta di un sistema che intercetta il flusso dati in partenza ed in arrivo da e verso l'utente, che offre la possibilità di ricostruire in modo intelligibile i segnali analogici della comunicazione tra i modem, e che si colloca sulla linea telefonica dell'utente "a metà strada" tra l'utente stesso ed il provider. Accade però che tale sistema venga messo "fuori gioco" tutte le volte in cui l'indagato utilizzi per la connessione una linea telefonica diversa da quella consueta. In questo caso, gli stessi dovranno essere inseriti su più linee e punti come osservatori.

4.4.b) segue: Le intercettazioni telematiche in materia di indagini contro la pedo-pornografia.

La lotta allo sfruttamento sessuale dei minori, pur essendo condotta su più fronti, si sta rivelando particolarmente fruttuosa in virtù del sempre più efficace contrasto implementato sulle reti informatiche e telematiche. È una constatazione che non desta sorpresa: in un'epoca, come quella attuale, contrassegnata dal rapido e spesso invadente progresso tecnologico; era inevitabile infatti che anche i responsabili di attività delittuose riconoscessero nei moderni mezzi di telecomunicazione, e in particolare in internet, un comodo canale per l'organizzazione e la gestione dei loro traffici. Le potenzialità, invero, sono ragguardevoli: si pensi alla rapidità dello scambio dei dati, alla capillare diffusione dello strumento e allo stesso anonimato, sia pure non sempre insuperabile, assicurato dalla rete. Date queste premesse, appariva scontata la predisposizione di strumenti investigativi che scendessero sullo stesso terreno. Di qui l'introduzione, potremmo dire "speculare", degli strumenti di contrasto contemplati dall'***art. 14 della l. 3 agosto 1998, n. 269.***

Detta disposizione comprende due dstinti istituti che derivano la loro efficacia dal fatto di fare ricorso alle modalità investigative proprie delle attività cosiddette sotto copertura.

Il comma 1 prevede infatti che, nell'ambito di operazioni disposte dal questore o dal responsabile di livello almeno provinciale dell'organismo di appartenenza, gli ufficiali di polizia giudiziaria in forza a strutture specializzate, al solo fine di acquisire elementi di prova in ordine a taluni delitti (segnatamente quelli puniti dagli artt.600 *bis* comma 1[prostituzione minorile] , 600 *ter* commi 1, 2 e 3 [pornografia minorile] e 600 *quinquies* [iniziative turistiche volte allo sfruttamento della prostituzione minorile] c.p.), possano procedere, previa autorizzazione dell'autorità giudiziaria, all'acquisto simulato di materiale pornografico, alle relative attività di intermediazione e

prendere parte ad iniziative turistiche volte allo sfruttamento della prostituzione minorile. **Il comma 2** attribuisce all'organo del Ministero dell'Interno preposto alla sicurezza e regolarità dei servizi di telecomunicazione, nell'ambito di compiti definiti da apposito decreto, il potere di svolgere le *"attività occorrenti per il contrasto"* delle medesime precedenti fattispecie criminose, allorquando siano commesse mediante l'impiego di sistemi informatici, mezzi telematici o reti di telecomunicazione disponibili al pubblico. Rigorose le condizioni - sovrapponibili, come detto, a quelle contemplate per le operazioni cui al comma 1 - occorrendo, anche in tal caso (e, si ripete, per le medesime fattispecie delittuose), la richiesta dell'autorità giudiziaria motivata a pena di nullità, e la particolare qualificazione del personale che deve essere specializzato. Le modalità operative non sono indicate con pari precisione, in modo tale che si adattino alle molteplici esigenze investigative e alle trasformazioni tecnologiche che possono intervenire nella rete. Tra le predette modalità si possono comunque annoverare tutti quegli espedienti volti a dissimulare specifiche operazioni di polizia, mascherate con indicazioni di copertura, anche attraverso la creazione di siti c.d. "civetta"; la realizzazione o gestione di aree di comunicazione o scambio di informazioni o, ancora, la partecipazione attiva a queste ultime.

Nei predetti casi, il sito (o la parimenti artificiosa area di scambio di opinioni *on line*) creato *ad hoc* dagli organismi investigativi deve essere continuamente monitorato ed aggiornato aggiungendovi, se del caso, riflessioni ed esperienze, pure con spunti "polemici".

La costruzione del sito sotto l'aspetto tecnico deve essere quindi curata con molta attenzione, atteso che l'attività sotto-copertura avviata deve risultare "credibile" e preordinata al reperimento di dati ed operazioni poste in essere dai visitatori e dagli iscritti (e poterli così successivamente identificare).

Anche il nome del sito pertanto deve essere studiato con grande precisione e accuratezza, dato che deve inserirsi adeguatamente nell'ambiente "pedo-culturale" o pedofilo. A tal fine potrà risultare altresì utile relazionarsi con i semplici visitatori del sito nella veste scriminata di "*agente provocatore*"e ciò allo scopo di riuscire a reperire dettagliate informazioni sulle attività abitualmente esperite dai frequentatori di tali ambienti e sui loro comportamenti ricorrenti.

Ora, l'operatività degli istituti cui alle previsioni dei commi 1 e 2 del citato articolo 14 della L. n°269 del 1998 è limitata, come evidenziato *supra*, ad un nucleo ristretto (e coincidente nei due casi) di reati.

Una simile opzione indica la comprensibile preoccupazione del legislatore di non dilatare eccessivamente il ricorso a tali istituti, per riservarli alle figure delittuose di maggiore offensività e pericolosità. La predetta scelta di politica criminale tuttavia non manca di dar luogo – come evidente - a qualche incertezza esegetica. Non è chiaro, ad esempio, quali effetti conseguano ad un'operazione che, pur compiuta nel rispetto di tutti i presupposti normativi, ivi compreso quello teleologico, conduca alla scoperta di elementi rilevanti per una fattispecie incriminatrice diversa da quelle tassativamente considerate (cioè, si ripete, quelle cui all'art. 600 *bis* co.1; art. 600 *ter* co. 1, 2 e 3 ed art. 600 *quinquies* c.p.), come, ad esempio, quelle di cui agli artt. 600-

ter comma 4 ovvero 600-quater c.p.[251]. E ancora, come conciliare l'esperibilità dei due istituti in esame con le nuove norme introdotte dalla legge 1 ottobre 2012 n°172 che ha dato - da ultimo - attuazione alle disposizioni contenute nella *Convenzione del Consiglio d'Europa* (nota come Convenzione di Lanzarote) *per la protezione dei minori contro ogni forma di abuso e di sfruttamento sessuale"* ? [252]

E' evidente, infatti, come il ricorso agli strumenti investigativi predisposti dall' art. 14 L. n°269/98 (soprattutto dal 2° comma) possa condurre gli inquirenti ad imbattersi con accentuata frequenza – estrinsecandosi in azioni propedeutiche e preliminari all'effettivo e concreto sfruttamento sessuale del minore – in condotte pienamente rientranti nell'ambito di operatività delle previsioni delle due nuove norme incriminatrici. Se poi si osservi come lo stesso art 609 *undecies* c.p. contempli tra le modalità di attuazione dell'adescamento proprio il ricorso a strumenti di comunicazioni basati sulle più moderne tecnologie digitali ed informatiche, si intuisce come gli eventuali risultati delle investigazioni ex art. 14 l. 269/98 dovrebbero poter essere spendibili nella successiva fase dibattimentale e portare all'aquisizione di elementi di prova proficuamente utilizzabili a carico dei soggetti accusati delle relative condotte. In caso contrario, lo strumento predisposto dal legislatore nel dare attuazione alla Convenzione di Lanzarote, assumerebbe le caratteristiche dell'arma spuntata e non riuscirebbe – fuori dai casi in cui le tradizionali intercettazioni di comunicazioni telematiche si mostrassero da sole sufficienti – a garantire una adeguata tutela contro le più subdole forme di adescamento osservabili oggi sulla Rete[253].

---

[251] Costituiscono espressione di questa incertezza interpretativa, le oscillanti ed ondivaghe pronunce sul punto della Giurisprudenza di legittimità. Ex plurimus: Cass. Sez. III, 3 dicembre 2001, D'Amelio, in Giur. it., 2003, p. 545; Cass. Sez. III, 8 maggio 2003, Busi, in Guida dir., n. 50, p. 68; Cass. Pen. Sez. III, 05 maggio 2005; Marinelli; Cass. Sez. III, 8 giugno 2004, Ganci;

[252] La predetta legge infatti, attraverso il meccanismo della novella al codice penale (e, per alcuni aspetti, al codice di rito), introduce due inedite ipotesi delittuose: l'art.414-bis c.p. (Istigazione a pratiche di pedofilia e di pedopornografia) - che menziona espressamente per la prima volta nel nostro ordinamento penale la parola pedofilia - stabilendo: *"Salvo che il fatto costituisca piu' grave reato, chiunque, con qualsiasi mezzo e con qualsiasi forma di espressione, pubblicamente istiga a commettere, in danno di minorenni, uno o piu' delitti previsti dagli articoli 600-bis, 600-ter e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-quater e 609-quinquies e' punito con la reclusione da un anno e sei mesi a cinque anni. Alla stessa pena soggiace anche chi pubblicamente fa l'apologia di uno o piu' delitti previsti dal primo comma. Non possono essere invocate, a propria scusa, ragioni o finalita' di carattere artistico, letterario, storico o di costume"*; e l'art. 609 *undecies* c.p. in base al quale: *"Chiunque, allo scopo di commettere i reati di cui agli articoli 600, 600-bis, 600-ter e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-quater, 609-quinquies e 609-octies, adesca un minore di anni sedici, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a tre anni. Per adescamento si intende qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione".*

[253] Si pongono, quindi, questioni esegetiche non difformi, a ben guardare, da quelle adombrate *supra* in relazione all'esperibilità (incidentalmente) delle operazioni sotto-copertura al di fuori del ristretto ambito previsto dalla norma con riferimento, in particolare, all'utilizzabilità degli elementi di prova

Peraltro, a prescindere da quale sia l'opzione ermeneutica da preferirsi in ordine alle anzidette questioni e tralasciando, *de iure condendo*, le considerazioni circa gli auspicabili interventi normativi (per lo più in chiave di coordinamento fra istituti già esistenti) necessari al fine di dare maggiore incisività nel nostro ordinamento alle norme che recepiscono la Convenzione di Lanzarote, è di tutta evidenza come lo strumento d'indagine "principe" in materia di pedo-pornografia - proprio alla stregua delle considerazioni svolte in apertura di paragrafo - sia senz'altro costituito dalle intercettazioni di flussi di comunicazioni relativi a sistemi informatici e telematici.
In relazione al predetto strumento, in particolare, il protocollo investigativo più utilizzato consiste nella previa individuazione - a cura della P.G. - di una serie di siti pedo-pornografici (italiani ed esteri), scelti tra quelli che per numero e qualità delle immagini offerte presentano maggiore pericolosità. Si procede, quindi, all'intercettazione telematica sui fasci di dati diretti dall'Italia a tali siti (*c.d. intercettazioni parametriche*), con un tabulato periodico riportante tutte le *login name* degli utenti che hanno avuto accesso a tali siti attraverso il *server* locale ("pop") di un *provider* italiano.
Viene quindi realizzata, sulla base dei dati in ingresso, una sorta di statistica di "frequenza di accesso" degli utenti che hanno visitato detti siti e, alla stregua di questa, si potrà verificare, quali siano gli utenti con maggiore densità di traffico.
Su di essi si avvierà una intercettazione mirata, tesa a catturare tutto il traffico dati generato da tali utenti da e verso il sito incriminato. L'intercettazione così disposta consentirà di avere copia di tutte le informazioni transitate da e per il sito durante ogni "sessione" di collegamento dell'utente, con l'esatta riproduzione delle operazioni da lui compiute e delle specifiche immagini visualizzate e scaricate sul suo computer.

4.4.c) Intercettazioni in rete e connessioni a sistemi informatici ubicati all'estero.

Ogni utente che si colleghi ad Internet per svolgere qualsiasi attività in rete (navigare tra i siti, inviare posta elettronica, *chattare* o partecipare a *newsgroup*), di norma svolge tali attività transitando dal *server* di un *provider* il cui nodo di trasmissione (cd. *pop*) si trova fisicamente nei pressi del luogo da cui chiede la connessione.
In questi casi, partendo da quella connessione, potrà sì visitare siti e sistemi sparsi su tutta la Terra, ma pur sempre utilizzando una **linea telefonica italiana**: cosicché – la cosa è di tutta evidenza - i flussi che passeranno da quella utenza potranno essere lecitamente intercettati secondo la disciplina italiana sulle intercettazioni.

---

eventualmente acquisiti (e la legittimità dei correlativi sequestri) all'interno di giudizi, successivamente instaurati, per l'accertamento di reati differenti da quelli contemplati dalla L. n°269 del 98 (benché si tratti di reati aventi sempre la stessa indole quali quello previsto e punito dai nuovi artt. 414 *bis* e 609 *undecies* c.p.).

Scopo dell'intercettazione è, d'altra parte, prelevare in tempo reale dei dati durante il loro fluire su di un canale di trasmissione e ricostruirne i contenuti in modo da renderli perfettamente fruibili agli investigatori. Ora, mentre queste fasi erano pressoché banali ed intuitive per le intercettazioni telefoniche su linea analogica, divengono complesse e difficili da inquadrare (anche sotto il profilo giuridico) nell'ambito delle comunicazioni digitali.

Esistono infatti diversi livelli di intercettazione digitale e ciò proprio per il fatto che la "Rete delle reti" opera in maniera stratificata, ossia impiega *layer* che sono il più possibile permeabili tra loro per ragioni di convenienza economica e tecnica.

Ad analoghe conclusioni, peraltro, potrà giungersi anche nel caso in cui l'utente in questione utilizzi l'accesso alla rete fornito dal server di un ***provider*** **fisicamente collocato all'estero** (ad es. British Telecom).

Tutte le volte in cui, infatti, la chiamata per l'estero parta da un'utenza collegata ad una centrale telefonica sita nel territorio italiano, ovvero nei casi in cui dall'estero arrivi una chiamata per un'utenza sita nel territorio dello Stato e venga pertanto smistata ancora una volta da una centrale "italiana", l'intercettazione sarà ovviamente consentita secondo i normali strumenti processuali, senza che sia necessario, quindi, richiedere alcuna forma di assistenza rogatoriale all'estero.

Sul punto la Corte di Cassazione[254] si è definitivamente pronunciata ritenendo che non si verifichi alcuna violazione dell' art. 267 c.p.p. in relazione all'art. 271 dello stesso codice nel caso di intercettazioni telefoniche internazionali così articolate, a patto che le intercettazioni medesime riguardino un'utenza sita in territorio italiano dalla quale vengano fatte telefonate all'estero, ovvero abbiano ad oggetto telefonate che da un'utenza straniera arrivino in Italia. In realtà, le diverse decisioni della Suprema Corte sul punto hanno riguardato specificamente ipotesi di intercettazioni (in entrata o in uscita) su numeri telefonici internazionali e, quindi, essenzialmente intercettazioni telefoniche *stricto sensu.* Ciò, tuttavia, non impedirebbe di estendere la portata e gli effetti delle svariate pronunce sull'argomento anche alle intercettazioni telematiche le quali, del resto, si caratterizzano - differenziandosi per questa via dalle intercettazioni informatiche propriamente dette - per il fatto di concernere dispositivi digitali messi in comunicazione fra loro ricorrendo alle molteplici soluzioni offerte oggi dalla tecnologie delle telecomunicazioni.

Ad incardinare la competenza territoriale italiana sarà quindi sufficiente che almeno uno dei due "capi" della comunicazione sia fisicamente collocato in Italia, cosicché essa debba necessariamente transitare su un "nodo" telefonico della rete italiana.

E' quindi intercettazione "italiana" quella che ha per oggetto tutte le comunicazioni in entrata (anche dall'estero) su un'utenza del territorio nazionale, nonché le comunicazioni che, partendo da una simile utenza, siano dirette all'estero: *"Non comporta violazione delle norme sulle rogatorie internazionali l'intercettazione di telefonate in partenza dall'Italia e dirette all'estero, in quanto tutta l'attività di*

[254] Cfr. *infra.*

intercettazione, ricezione e registrazione delle telefonate viene compiuta interamente sul territorio italiano[255]*.*

Nella medesima citata sentenza la Corte ha altresì precisato che in tale predetta ipotesi non è necessaria la tecnica dell'istradamento-convogliamento delle chiamate in partenza dall'estero in un "nodo" posto in Italia, *in quanto la captazione ha ad oggetto una comunicazione che non solo transita, ma ha origine sul territorio nazionale, per cui il contatto con un'utenza straniera è del tutto occasionale e non prevedibile";* Del medesimo tenore è anche la, quasi coeva, sentenza della Sez.VI, n. 7258 del 02/11/2004 secondo cui: *"In tema di intercettazione di comunicazioni o conversazioni, è legittima l'utilizzazione della* ***tecnica del cosiddetto istradamento****, che comporta la destinazione ad uno specifico "nodo" telefonico delle telefonate estere provenienti da una determinata zona, senza che venga promossa una apposita rogatoria internazionale, posto che l'intera attività di captazione e registrazione si svolge sul territorio dello Stato.* In motivazione la Corte ha altresì precisato che la tecnica, posto che il provvedimento autorizzativo estende implicitamente i propri effetti a tutte le operazioni strumentali*, non comporta l'intercettazione illegale di chiamate concernenti utenze non sottoposte ad indagine, e consiste in una semplice forma di attuazione del controllo, tanto che la sua utilizzazione non richiede indicazioni formali del P.M.*.

4.5 La cooperazione giudiziaria e di polizia in materia di *cybercrime*.

4.5.a) Premessa.

Lo sviluppo delle tecnologie dell'informazione e , soprattutto, delle comunicazioni via internet, ha determinato, come più volte messo in evidenza *supra*, un rapidissimo cambiamento dell'organizzazione della società mondiale, modificando in profondità la struttura ed il funzionamento di fondamentali settori della vita economica e sociale.

La svolta è stata indubbiamente segnata dal progressivo sviluppo della possibilità di accesso a tali mezzi che, essendo ormai alla portata di una vasta parte della popolazione mondiale, consentono di elaborare, memorizzare e diffondere dati ed informazioni con una velocità e semplicità inimmaginabili solo fino a pochi anni fa.

Sono emersi, pertanto, nuovi rilevanti problemi d'integrazione culturale, di bilanciamento di diversi e contrastanti interessi e di disciplina giuridica di nuovi tipi di fatti e condotte non più sussumibili nelle tradizionali categorie giuridiche, mettendo in grave evidenza l'inadeguatezza degli attuali sistemi giuridici nazionali ed internazionali rispetto alle insidiose sfide poste dal *cybercrime*.

[255] Cass. IV, n. 37646 del 30/06/2004.

Si evidenzia oggi più che mai, pertanto, la necessità di agire in plurime direzioni, quali:

- l'armonizzazione degli ordinamenti penali degli stati nazionali sotto il profilo sostanziale e processuale;
- lo sviluppo di una politica condivisa di cooperazione giudiziaria;
- la collaborazione con gli imprenditori privati del settore;
- la messa a punto di tecniche e strumenti investigativi idonei a fronteggiare la rapidità e diffusività delle condotte dei *cybercriminali*.

L'elemento di novità emerso con la diffusione del *web* - cioè la creazione di un nuovo spazio caratterizzato da moduli spazio-temporali globalizzati ove possono realizzarsi le più disparate condotte umane, lecite ed illecite, ed ove le stesse perdono il tradizionale rapporto di fisicità che avevano con elementi quali il luogo o il tempo – fa entrare in crisi il tradizionale concetto di sovranità degli ordinamenti e la loro pretesa di regolare autonomamente le manifestazioni umane verificatesi sul proprio territorio, potendo nel cyberspazio un'azione criminosa essere ideata e concordata in uno stato, eseguita attraverso delle apparecchiature site in uno o più stati differenti e produrre i propri effetti in altri Stati ancora.

A fronte di ciò, vanno sicuramente ripensati i processi di ideazione ed attuazione delle politiche criminali; così come si deve prestare la massima attenzione alla tutela di tutti gli interessi in gioco, bilanciando attentamente le esigenze di prevenzione e sicurezza con la dovuta tutela ai diritti fondamentali - tradizionali e nuovi - che oggi vengono esercitati anche attraverso l'accesso al *web*.

4.5.b) La cooperazione giudiziaria nelle indagini internazionali in materia di *cybercrime*.

Un primo, incipiente, passo in direzione di una maggiore consapevolezza delle azioni necessarie per "acconciare" sistemi e discipline - su scala globale - dei diversi ordinamenti al fine di pianificare e realizzare un più efficace contrasto dei fenomeni di *cybercrime* lo si è esperito, innanzitutto, attraverso la *Convenzione di Bruxelles del 29 marzo 2000 sull'Assistenza Giudiziaria in materia Penale* che contempla, infatti, una collaborazione (internazionale) celere ed informale tra i molteplici paesi aderenti, anche con riferimento alle indagini informatiche.

Ma è stato soprattutto il Consiglio d'Europa - attraverso l'adozione della Convenzione di Budapest del 23 novembre 2001 sul *cybercrime* - ad avere agito, in una cornice internazionale, in modo ancor più sistematico ed incisivo sul fronte del contrasto, a livello globale, ai crimini *cybernetici*, nella consapevolezza peraltro della duplice esigenza, da un lato, di non imbrigliare in regole eccessivamente rigide un mondo come quello della rete caratterizzato, per sua stessa natura, dal massimo livello di libertà di circolazione delle idee e delle informazioni e, dall'altro, di evitare che vi fossero paesi individuabili come *"paradisi del cybercrime"*, sul modello di quelli già

preferiti dai criminali come basi per il riciclaggio di denaro sporco grazie alle garanzie assicurate dalle legislazioni nazionali.
Ciò premesso, gli obiettivi fondamentali della Convenzione di Budapest si possono agevolmente riassumere nei seguenti tre punti:
1) armonizzare gli elementi fondamentali delle fattispecie di reato nell'ambito del diritto penale sostanziale degli ordinamenti nazionali e tutte le altre disposizioni connesse alla disciplina della *cyber* criminalità (artt. 2-13);
2) dotare le procedure penali dei paesi sottoscrittori dei poteri necessari a svolgere indagini efficaci e ad assicurare l'utile raccolta della prova penale, sia in materia di *computer crimes*, che in relazione ad ogni altro reato commesso mediante l'uso di mezzi di alta tecnologia dell'informazione e comunicazione
(artt. 14-22);
3) attuare un efficace e rapido *regime di cooperazione internazionale* in materia, tramite lo snellimento degli strumenti di assistenza (giudiziaria e di polizia) e lo scambio di informazioni e dati *in tempo reale* (artt. 23-35).
Per quanto concerne in particolare quest'ultimo punto, è di tutta evidenza come i fattori fondamentali per il successo di un'indagine in materia di *cybercrime* a dimensione internazionale siano rappresentati dalla velocità degli atti investigativi e dalla raccolta dei dati secondo le regole dell'ordinamento penale nazionale ove le prove debbono essere fatte valere. Nella consapevolezza di tali presupposti, la convenzione sul *Cybercrime*, nel porre i principi generali della materia, si ispira al massimo favore per la cooperazione internazionale, stabilendo all'art. 23 che *"le parti devono cooperare tra loro nella misura più ampia possibile nelle indagini o nei procedimenti riguardanti reati collegati a sistemi e dati informatici, o per raccogliere le prove, in forma elettronica, di un reato, in conformità alle disposizioni di questo capitolo e in applicazione degli strumenti internazionali sulla cooperazione in materia* penale, *degli accordi stipulati sulla base di una legislazione uniforme o in condizione di reciprocità e del loro diritto nazionale".*
In attesa e nella prospettiva di realizzare una cooperazione internazionale effettivamente corrispondente agli impegni assunti nei trattati internazionali menzionati sopra, sembra imprescindibile un approccio pragmatico che si fondi su alcuni punti fermi quali:
1) il *rapporto diretto tra autorità giudiziarie*, non mediato né rallentato da autorità politiche;
2) la *velocità della cooperazione*, che in fase di indagini deve adeguarsi alla velocità dei criminali;
3) l'*assenza* (quasi totale) di *formalità*.
Invero un'efficace azione di contrasto al *cybercrime* non può prescindere dalla cooperazione dinamica tra le Magistrature e le Forze di Polizia e tra le prime e le seconde che deve partire già dal momento iniziale delle indagini in tema di reati informatici,
Ci si riferisce non all'attività rogatoriale classica, alla tradizionale richiesta di prove e/o di svolgimento di attività investigativa, bensì al quotidiano, velocissimo,

frenetico, si potrebbe dire, scambio di dati e notizie tra Autorità Giudiziarie e tra Polizie Giudiziarie di Stati diversi nel corso delle indagini.

Tale *cooperazione dinamica* (come anche potremmo definirla), si propone di svolgere insieme le indagini mentre i fatti avvengono, al fine di poter ragionevolmente arrivare ad un risultato investigativo completo, con la ricostruzione precisa e dettagliata dei fatti-reato oggetto delle indagini e con l'accertamento delle eventuali responsabilità penali di tutti i protagonisti del crimine perseguito; risultato investigativo ben difficile da realizzare altrimenti e che sarebbe destinato ad esaurirsi in una richiesta di archiviazione per essere gli autori dei fatti rimasti ignoti (in quanto non identificabili all'estero), ovvero, nella migliore delle ipotesi, che si limiterebbe all'identificazione ed alla celebrazione del processo soltanto nei confronti dei soggetti che agiscono all'interno del proprio Stato, lasciando che altri, operando in altri Stati, possano continuare a delinquere indisturbati e, quel che è peggio, impuniti.

Una fattiva ed efficace cooperazione internazionale permette, quindi, di perseguire i due seguenti rilevantissimi risultati:

1) in primo luogo, consente di comprendere e conoscere a fondo fenomeni criminali dei quali, altrimenti, quasi neppure si sospetterebbe l'esistenza, e di raccogliere prove sull'intera catena criminale senza soffermarsi sul singolo anello che ha agito in Italia[256] o, comunque, nel singolo Stato.
2) in secondo luogo, l'azione repressiva ha una maggiore efficacia, in quanto gli Stati interessati, che vengono messi al corrente delle indagini condotte in un altro Stato, agiscono direttamente nei confronti dei reati commessi sul loro territorio. Quest'ultimo è un profilo da non sottovalutare, e che va al di là della normale collaborazione internazionale: esso infatti più che a far condannare in contumacia i criminali che vivono ed operano all'estero (e che mai, con ogni probabilità, verranno estradati dai loro Paesi), mira alla effettiva punizione e al diretto contrasto della criminalità informatica transnazionale.

E' di tutta evidenza, infine, la necessità - affinché si possa convenientemente concretizzare detta *cooperazione dinamica* - che i rapporti fra i diversi Stati coinvolti nelle indagini siano improntati alla massima e convinta reciproca fiducia; fiducia senza la quale la stessa normativa internazionale finirebbe per rimanere lettera morta.

Il che implica l'opportunità di intensificare i rapporti diretti fra Stati; segnalando alla A.G. e/o alle forze di Polizia appartenenti allo Stato interessato dalle indagini -

[256] Si pensi a fenomeni criminali di grande portata quali il *phishing*, le frodi o i sabotaggi di sistemi su larga scala, l'utilizzazione abusiva sistematica di carte di credito, le cd. *cyber*-estorsioni, il riciclaggio del denaro sporco attraverso i casinò virtuali, le aste *online*, l'*online banking* o la compravendita di titoli vari mediante transazioni elettroniche rapide ed anonime; la pedopornografia *online*, la prostituzione *online*, le truffe commerciali *online*, la contraffazione di beni realizzati e venduti tramite computer, le molestie informatiche (il c.d. *cyberstalking*), il gioco d'azzardo *online*, la riproduzione abusiva di programmi informatici o di ogni tipo di opera intellettuale su supporto digitale (libri, musica, film), l'accesso illecito a banchedati personali o la raccolta e la diffusione abusiva di tali dati (prelevati dai personal computers a mezzo dei *cookies* o di altro *spyware*); l'incitamento, l'istigazione o la trasmissione di istruzioni relative alla realizzazione dei più svariati crimini, il proselitismo terroristico *online*, ecc. ecc.).

previamente individuati attraverso gli organismi europei di coordinamento - i luoghi, ad esempio, in cui sono allocati i *server* che interessano; richiedendo loro i dati del traffico telefonico e/o telematico utili allo sviluppo delle indagini ed indicando le utenze telefoniche che è stato accertato essere in uso agli indagati. E ciò mediante attività inizialmente prive di particolari formalismi e preordinate ad innescare eventuali perquisizioni, ispezioni e sequestri informatici presso le società ove sono allocati detti *server*; o, ancora, a stimolare provvedimenti per l'acquisizione di dati del traffico telefonico e/o telematico presso i *provider*, intercettazioni, pedinamenti e quant'altro possa essere utile per il buon esito delle indagini. Con il rilevantissimo risultato, peraltro, che da quel momento in avanti tutti gli investigatori saranno a conoscenza, nel dettaglio, delle indagini e saranno in grado di ricostruire fedelmente il fatto che ne occupa, risalendo con certezza alle eventuali responsabilità.
Naturalmente, in assenza di specifiche norme convenzionali internazionali vincolanti per gli Stati coinvolti, i risultati investigativi così prodotti, ai fini della loro producibilità in giudizio, andranno formalmente acquisiti utilizzando gli strumenti rogatoriali previsti dalle leggi vigenti nei singoli ordinamenti.

4.5.c) segue: l'istituzione della Procura Europea.

In ambito squisitamente europeo[257], peraltro, i tempi per porre in essere il predetto modello di *cooperazione dinamica* fra organi inquirenti di differenti paesi, sembrano ormai maturi. Il Trattato sul Funzionamento dell'Unione Europea (TFUE) siglato a Lisbona nel dicembre del 2007 ed entrato in vigore il I gennaio 2009, prevede, infatti, all'art. 86, la possibilità che l'Unione, attraverso una procedura legislativa *ad hoc*[258], si doti di un inedito organismo investigativo preposto a individuare, perseguire e rinviare a giudizio - eventualmente in collegamento con Eurojust ed Europol - gli autori di reati che ledano gli *interessi finanziari dell'Unione*[259] e i loro complici. Detto organismo – testualmente definito Procura Europea – oltre a tutelare gli interessi finanziari dell'Unione, dovrebbe essere deputato, altresì, a perseguire tutti i più gravi fatti di criminalità aventi dimensione transnazionale, dinanzi agli organi giurisdizionali dei singoli Stati membri.
Ora, a distanza di oltre quattro anni dall'entrata in vigore del Trattato di Lisbona, e precisamente il 17 luglio del 2013, la Commissione europea ha avviato l'anzidetto *iter* normativo finalizzato alla istituzione del predetto ufficio di Procura.
Nelle sue dichiarazioni programmatiche il Presidente della Commissione *pro tempore* ha auspicato che il nuovo organismo possa iniziare a funzionare già dal I gennaio del

[257] Con la sola eccesione di U.K. e Danimarca e con l'*option (in o out)* da esperirsi da parte dell'Eire.
[258] Stessa procedura "aggravata" prevista dal successivo art. 87 TFUE al fine emanare norme di diritto europeo tese a sviluppare, tra le diverse autorità di polizia degli stati aderenti, una cooperazione di tipo operativa e non meramente di interscambio informativo e/o addestra.
[259] Definiti da apposito regolamento.

2015 e che possa colmare, in modo definitivo, le divergenze sussistenti tra i diversi sistemi penali degli Stati membri.
La proposta di regolamento – COM (213) n°534 – delinea, nello specifico, un ufficio di Procura Europeo secondo un modello decentrato destinato ad intergrarsi nei sistemi giudiziari nazionali. Più precisamente, a fianco della figura del Procuratore, nominato dal Consiglio previa consultazione del Parlamento europeo, vengono previsti quattro procuratori aggiunti (o delegati) e cinque sostituti procuratori. Questi eserciteranno le proprie funzioni nella duplice veste di magistrati europei e di pubblici ministeri nazionali. I procuratori delegati, quindi, eseguiranno indagini ed avvieranno azioni penali nello Stato membro cui saranno assegnati avvalendosi, a tal fine, del personale nazionale e applicando le leggi del singolo Stato. I predetti magistrati saranno diretti e coordinati dal procuratore europeo il quale, attraverso il suo puntuale intervento, assicurerà uniformità di approccio in tutta l'Unione e, se del caso, potrà altresì decidere di avocare direttamente l'effettuazione delle indagini servendosi, per il loro concreto espletamento, delle autorità di polizia nazionali. Sulla base dei suoi ampi poteri, il Procuratore, al verificarsi di specifiche esigenze, potrà addirittura sottrarre la direzione delle indagini al sostituto a cui inizialmente le stesse erano state assegnate ed affidarle ad altro sostituto anche se operante in uno Stato diverso.
La proposta in esame conferisce, inoltre, alle persone indagate dalla Procura europea diritti procedurali più estesi rispetto a taluni sistemi nazionali garantendo, in ogni caso, il diritto alla traduzione e all'interpretazione, il diritto all'informazione e all'accesso agli elementi di prova oltre che il diritto a farsi assistere da un avvocato in caso di arresto.
Le norme proposte, oltre a delineare questa prima fisionomia della Procura europea definiscono, altresì, taluni diritti che la legislazione dell'UE non ha tutt'ora armonizzato e rafforzano ulteriormente i diritti procedurali degli indagati. Tra questi, il diritto a tacere e la presunzione di innocenza; il diritto al patrocinio a spese dello Stato e il diritto di presentare elementi di prova a proprio discarico ovvero di chiedere l'audizione di testimoni.
La proposta definisce inoltre norme chiare e armonizzate sulle misure investigative che la Procura europea può disporre per le sue indagini e disciplina la raccolta e l'utilizzo degli elementi di prova.
Così, ad esempio, nei casi di indagini che concernono reati di una certà gravità che coivolgono più Stati dell'Unione, il Procuratore europeo potrà promuovere il coordinamento fra più sostituti procuratori europei e fra le varie autorità inquirenti e di polizia nazionali delegate allo svolgimento delle indagini, così come potrà decidere di seguire in prima persona le investigazioni.
Di notevole rilievo, inoltre, la disposizione introdotta dall'articolo 25 della proposta di regolamento nella quale si legge chiaramente che, *"ai fini delle indagini e dell'esercizio delle azioni penali ad opera dell'ufficio del Procuratore europeo, l'intero territorio degli Stati membri dell'Unione deve essere considerato alla stregua di un'unica area legale all'interno delle quale il Procuratore può esercitare le sue prerogative e le sue legittime funzioni senza particolari limitazioni".* Qualora si

rendesse poi necessario richiedere – per caratteristiche intrinseche alle azioni delittuose - la cooperazione di uno Stato terzo, la proposta di regolamento assegna al Procuratore ampi poteri di coordinamento e peculiari strumenti giuridici necessari per richiedere assistenza e collaborazione alle autorità inquirenti extracomunitarie.
Dal punto di vista dei mezzi necessari per la ricerca delle fonti di prova, la proposta riconosce alla Procura europea – come si accennava *supra* - un ventaglio molto ampio e penetrante di strumenti investigativi. Tra i predetti strumenti (da esperirsi alla stregua delle norme dello Stato di esecuzione) si annoverano: ispezioni; perquisizioni; sequestri; ordini di esibizione; accesso a corrispondenza e documentazione; intercettazioni di comunicazioni informatiche e telematiche; accesso alle banche dati relative alle transazioni economiche e finanziarie; controllo della documentazione custodita dagli istituti di credito e dalle società finanziarie; il potere di autorizzare operazioni sotto-copertura e video-riprese in luoghi non aperti al pubblico (con l'esclusione delle abitazioni private); la capacità di disporre pedinamenti, anche mediante il tracciamento gps e l'identificazione di sospetti attraverso il rilevamento di dati biometrici e pose fotografiche; la facoltà di ordinare consulenze tecniche, rilievi, sopralluoghi, campionature e di interrogare o far interrogare indiziati e potenziali testimoni. Infine il Procuratore europeo viene legittimato dalla proposta di regolamento ad attivare presso le autorita giudiziali competenti l'esecuzione di misure restrittive e interdittive o di richiedere l'attuazione di misure cautelari anche di natura custodiale.
Ovviamende, come anticipato in apertura, il coordinamento (ma sarebbe più corretto parlare di univocità) dell'azione investigativa sarà possibile nei limitati casi contemplati dallo statuto del Procuratore europeo[260].
Ciò non toglie peraltro che, fenomeni criminali di vasta portata quali: il *phishing*, le frodi o i sabotaggi di sistemi su larga scala; l'utilizzazione abusiva sistematica di carte di credito; le cd. cyber-estorsioni, il riciclaggio del denaro sporco attraverso i casinò virtuali; la pedopornografia e la prostituzione *online*; le truffe commerciali e bancarie *online* ecc. ecc. – giusto per citarne alcuni – costituiscono eventi delittuosi di accentuata pericolosità che ben si presentano quali fonte di grave e rilevante pregiudizio per gli interessi finanziari dell'Unione. A ciò si aggiunga che le predette attività, molto spesso, vengono ideate e poste in essere da temibili organizzazioni criminali, presentando, ontologicamente e per la loro stessa architettura, non soltanto carattere transfrontaliero, ma un'effettiva e preoccupante dimensione sovranazionale. Va da se che, in ordine ai predetti casi e al ricorrere di consimili gravi eventi criminali - posti in essere attraverso il disinvolto sfruttamento di tecnologie informatiche e telematiche - l'intervento del Procuratore europeo si rivelerà non soltanto desiderabile, ma addirittura inevitabile e doveroso.

[260] In definitiva escludsvamente nelle ipotesi in cui siano pregiudicati gli interessi finanziari della U.E. ovvero nei casi di gravi forme di criminalità transfrontaliera.

4.5.d) Le linee guida di cooperazione tra le Forze di Polizia e gli Internet Service Providers contro i cybercrimes.

In attesa che, *de iure condendo*, si ponga mano (anche in ambito ultra-europeo) ad un complessivo e sistematico progetto di regolamentazione teso a disciplinare non soltanto i rapporti tra organi inquirenti di diversi stati, ma anche le relazioni che inevitabilmente si pongono fra quest' ultimi e gli Internet Service Provider appartenenti a differenti nazioni, il contrasto al *cybercrime* si avvale, ancora, delle *"linee guida di cooperazione tra le FF.PP e gli Internet Service Providers contro i reati informatici".* Queste costituiscono un *"documento"* volto ad additare, sotto forma di mere raccomandazioni prive di qualsivoglia valore normativo cogente, alcune linee guida di cooperazione tra la polizia giudiziaria e gli Internet Service Providers (ISP). Detto documento, adottato nell'aprile del 2008 a Strasburgo nell'ambito della Conferenza plenaria sulla cooperazione contro il *cybercrime*, viene scandito in tre segmenti principali, concernenti:

a) *le linee guida comuni,* con le quali, da un lato, si sollecita l'adozione da parte degli Stati Membri del Consiglio d'Europa di norme idonee a portare a completa attuazione quanto previsto sul punto dalla Convenzione di Budapest; dall'altro, invece, vengono richiamati i comuni doveri di cooperazione (tra FF.PP. e ISP) al fine di consentire un adeguato contrasto del *cybercrime*, nel rispetto dei diritti e delle prerogative, anche di rango costituzionale, dei singoli utenti. Tra le molteplici misure proposte, si sottolinea il continuo scambio di informazioni e conoscenze tecnico-giuridiche tra ISP e FF.PP. nell'ambito di frequenti incontri e seminari tesi ad analizzare peculiarità e tendenze dei fenomini criminali più diffusi in internet.

b) *Le incombenze in capo alla Polizia Giudiziaria* e, in particolare, l'adozione di idonea strumentazione tecnica che garantisca la ricezione, in tutta sicurezza, delle informazioni richieste agli ISP; la redazione di specifici protocolli che consentano all'ISP, tra l'altro, di verificare l'origine delle richieste di volta in volta pervenute; l'utilizzo della forma scritta nelle richieste ed il ricorso ad appositi *form standard* ricomprendenti i dati utili e comunque quelli considerati essenziali per l'ISP; la previsione che solo in casi di urgenza Ì'ISP terrà conto di richieste orali sempreché le stesse siano immediatamente seguite da una richiesta scritta. Si richiede inoltre che le Autorità di Polizia pongano mano ad un serio e continuo programma di aggiornamento del proprio personale da impiegare, in via esclusiva, al contrasto del *cybercrime*.

c) *Le misure che dovranno essere adottate dagli ISP* quali, ad esempio, la redazione di specifici protocolli scritti di assistenza alla Polizia Giudiziaria (comprensivi della indicazione della tipologia di dati che potranno essere resi disponibili); l'impegno a creare strutture che possano fornire assistenza, in caso di effettiva urgenza, anche al di fuori degli orari di ufficio e nei fine settimana; la precisa validazione dei dati forniti alla Polizia Giudiziaria (l'assicurazione cioè che i dati forniti alle Autorità siano completi, accurati e protetti); l'impegno a denunziare prontamente

alle FF.PP. ogni abuso o reato perpetrato sul *web* o in internet cui l'ISP sia venuto a conoscenza; l'assiduià nella formazione del proprio personale specificatamente designato ad intrattenere raporti di collaborazione con gli organi di polizia ecc. ecc.

Trattasi, come è evidente, di indicazioni di buon senso (c.d. *best practices*) pienamente condivisibili e da adottare senza tentennamenti al fine di pervenire al giusto contemperamento tra le esigenze investigative (spesso improntate verso una necessaria celerità nella risposta) e quelle volte a poter esercitare, soprattutto in sede difensiva, una effettiva verifica dei dati forniti dagli ISP e contestualmente acquisiti dalla Polizia Giudiziaria.

Le linee guida di cui si discute possono essere considerate, in ultima analisi, alla stregua di vere e proprie regole organizzative interne di cui possono dotarsi ISP e FF.PP. al fine di rendere più agevole e snella la vicendevole collaborazione in vista del contrasto al *cybercrime,* nel totale e reciproco rispetto delle prerogative e delle responsabilità di ciascuno e tenendo sempre presenti i fondamentali ed incolculcabili diritti degli utenti di internet.

Si evidenzia infine come la c.d. "Società dell'informazione" - quello spazio cioè tendenzialmente globale in cui gli individui possono liberamente creare, utilizzare e condividere informazioni e conoscenza al fine di migliorare la propria condizione e qualità di vita - non possa prescindere più, oggi, da nuove e più incisive forme di partenariato e cooperazione tra Governi, settore privato, società civile ed organizzazioni internazionali. Ed è fuor di dubbio che, in questa prospettiva, un ruolo cruciale sia giocato proprio dagli ISP e dalle Autorità legalmente preposte alla repressione degli abusi informatici.

Quanto precede, chiarisce in sostanza perché tra gli obiettivi programmatici delle *guidelines* figuri altresì l'auspicio che le stesse trovino contestuale ed estesa diffusione ed applicazione, a livello globale, in tutti i Paesi del mondo, nel rispetto dovuto alle legislazioni nazionali, alla libertà di espressione, alla privacy, ed in generale a tutti i diritti fondamentali dei *net-citizen*.

BIBLIOGRAFIA:

- Amodio, *Il processo penale tra disgregazione e recupero del sistema,* in Indice Penale 2003 pp. 7 e ss.;

- Amore – Stanca – Staro, *I reati informatici*, Halley editrici (MC), 2010;

- Antolisei, *Manuale di Diritto Penale, ed. 2011 – 2012;*

- Aprile, *Limiti alla utilizzabilità processuale del sequestro di materiale informatico acquisito mediante siti web "civetta"*, in Dir. Internet, 2005, 39;

- Aprile- Spiezia, Le intercettazioni telefoniche ed ambientali, Milano 2004;

- Aprile, *Le indagini tecnico scientifiche: problematiche giuridiche sulla formazione della prova penale*, Milano,2008

- Aterno, *Il legislatore interviene ancora sul data retention, ma non è finita,* in Dir. Pen. e Processo, 2009, 282;

- Aterno, *La computer forensics tra teoria e prassi: elaborazioni dottrinali e strategie processuali,* in Cyberspazio e diritto, 2006;

- Aterno in, Acquisizione e analisi della prova informatica, in Dir. pen. proc., 2008, Suppl. Dossier;

- Aterno, *In materia di sequestro di hard disc e acquisizione della prova informatica: un caso eclatante*, in Dir. internet, 2005, (2), p. 365 ss.;

- Aterno, *Le fattispecie di danneggiamento informatico*, in Luparia (a cura di), Sistema penale e criminalità informatica, Milano, 2009, p. 35 ss.;

- Balducci, *Le garanzie nelle intercettazioni tra Costituzione e Legge ordinaria*, Milano 2002;

- Barbieri, *Le attività di indagine della polizia giudiziaria sui sistemi informatici e telematici* in Dir. Internet 2008, 517;

- BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. Luparia (a cura di), Sistema penale e criminalità informatica, Milano, 2009, p. 181 ss.

- Braghò, *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa*, in Dir. Informaz. e Informatica, 2005, pp. 520 e ss.

- Bettoni, *Terrorismo e internet, alcune riflessioni,* in Cyberspazio e diritto 2010, 244;

- Bottà, *Google: l'indirizzo IP non identifica nessuno*, in Punto informatico, 26.02.2008;

- Bruno, *Intercettazione di comunicazioni o conversazioni*, in Dig. D. Penale, Tornino 1993, 181;

- Buonomo, *Metodologia e disciplina delle indagini informatiche,* in Profili penali dell'informatica, Milano 1994;

- Buonomo, *Profili penali dell'informatica*, Milano 1994, pg. 135 ss.;

- Caiani, *"I nuovi mezzi di ricerca della prova: videoriprese investigative, agente segreto attrezzato per il suono, pedinamento elettronico ed appostamenti informatici, installazione di captatori informatici*, in AA. VV. Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici, vol. II, Forlì, 2011, p. 443 ss.

- Caiani - D'Agostino - Vannin,*"Di necessità, virtù": appunti per una strategia globale al contrasto del cybercrime. l'esperienza del pool reati informatici della procura di Milano,* in IISFA Memberbook 2011 in Digital Forensics a cura di Costabile e Attanasio, Condivisione della conoscenza tra i membri dell' IISFA ITALIAN CHAPTER;

- Cajani – Costaile, *Information technologies in the criminal investigation: a European perspective,* Forlì 2011;

- Cajani, *Considerazioni sull'impatto della "distrettualizzazione"ex legge 48/2008 sul pool reati informatici della Procura di Milano*, in AA.VV., (a cura di Costabile, Attanasio), *IISFA Memberbook 2100 Digital Forensics*, Forlì, 2010, pp. 1 e ss.;

- Camon, *Le intercettazioni nel processo penale*, Milano 1997;

- Camon, *L'acquisizione dei dati sul traffico delle comunicazioni*, in Riv. it. dir. proc. pen., 2005, 605 ss. e 645 ss.

- Caprioli, *Le disposizioni in materia di intercettazione e perquisizione*, in AA.VV., Il processo penale tra politiche della sicurezza e nuovi garantismi, a cura di G. DI CHIARA, Torino, 2003, 4;

- Carnevale, in *Copia e restituzione dei documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in Dir. Pen. e Processo 2009 pp. 481 e ss.

- Cassano - Cimino, *Diritto dell'internet e delle nuove tecnologie telematiche*, Padova, 2009, p. 636.

- Cassibba, *L'ampliamento delle attribuzioni del pubblico ministero distrettuale in Luparia (a cura di) Sistema penale e criminalità informatica,* Milano 2009;

- Cajani, *La convenzione di Budapest nell'insostenibile salto all'indietro del legislatore italiano, ovvero quello che le norme non dicono…,* in Cyberspazio e diritto 2010, 185;

- Cajani, *Considerazioni sull'impatto della "distrettualizzazione" ex legge 48/2008 sul pool reati informatici della Procura di Milano, in AA.VV.*, (a cura di Costabile, Attanasio), IISFA Memberbook 2100 Digital Forensics, Forlì, 2010, pp.1 e ss.;

- Cajani - Costabile - Mazzaraco, *Phishing e furto d'identità digitale. indagini informatiche e sicurezza bancaria*, Giuffrè, 2008;

- Costabile - Rasetti, *Scena criminis, tracce informatiche e formazione della prova*, in Cyberspazio e diritto, 2003, vol. 4, n. 3/4, 273;

- Costabile, *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008*, in Ciberspazio e diritto, 2010, (3), p. 465 ss;

- Conte – Gemelli - Licata, *Le prove penali*, in Trattati a cura di Cedon, Giuffrè, 2009;

- CORDERO, *Il procedimento probatorio, in ID., Tre studi sulle prove penali*, Milano, 1963,

- Cuomo – Razzante, *La nuova disciplina dei reati informatici*, Giappichelli, Torino, 2009;

- D'Ambrosio, *Pratica di Polizia Giudiziaria*, Cedam Padova 2012;

- D'Aiuto – Levita, *I reati informatici: Disciplina sostanziale e questioni processuali*, Giuffrè, Milano, 2012;

- Destito – Dezzani - Santoriello, *Il diritto penale delle nuove tecnologie,* Cedam 2007;

- Dezzani, *Adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione,* in Riv. Guardia di Finanza, 2012, (3), p. 339 ss

- Diddi, *Ritocchi ad attribuzioni e competenze distrettuali*, in Scalfati (a cura di) Il decreto sicurezza, Torino, 2008, 147.

- Di Bitonto, *L'accentramento investigativo delle indagini sui reati informatici,* in Dir. Internet, 2008, 503;

- Di Ciommo, *Nota sulla Sentenza della Corte Federale USA del 29 giugno 2004,* in Foro It., 2004, IV, 449 e ss.;

- Di maria -Mignone, *I "cybercriminali": rischi e limiti dei profili criminologici,* in Ciberspazio e diritto, 2001, (2), p. 3 ss.;

- Di Martino, *Le intercettazioni telematiche e l'ordinamento italiano:una convivenza difficile,* in Indice Pen, 2002,219;

- Dominioni*, La prova penale scientifica*, Giuffrè 2005;

- Dominioni, *La catena di custodia e la genuinità della prova scientifica nel processo penale,* Novara, 2013;

- Dominioni, Nuova prova penale scientifica e regime di ammissione, Giuffrè 2011;

- Faggioli - Ghirardini, *Computer forensics: il panorama giuridico italiano*, in Ciberspazio e diritto, 2007, (3-4), p. 329 ss.

- Filippi, *L'intercettazione di comunicazioni,* Milano 1997;

- FILIPPI*, Terrorismo internazionale: le nuove norme interne di prevenzione e repressione. Profili processuali, in Dir. pen. proc., 2002, 167.*

- Flor, *Brevi riflessioni a margine della sentenza del BundesVerffassungsgericht sulla c.d. online DurchSuchung,* in Riv. Trim. di diritto pen. dell'economia, 2009, 695;

- Flor, *Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto,* in Dir. pen. proc., 2008, (1), p. 106 ss.;

- Flor, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet,* Verona, 2012;

- Fogliani, *Corso di informatica giuridica*, Milano 2009;

- Fondaroli, *La tutela penale dei beni informatici, in Diritto dell'informazione e dell'informatica*, 1996, pag. 316;

- Fulvi, *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica,* in Dir. pen. proc., 2009, (5), p. 639 ss.

- Fumu, *Commento al codice di procedura penale sub art. 266 bis*, Torino 1998;

- Furfaro, *Un problema irrisolto: le intercettazioni telefoniche, in Procedura penale e garanzie europee,* Torino, 2006, 120.;

- *Galantini, Inutilizzabilità della prova e diritto vivente in Rivista italiana di Diritto e Procedura Penale, 2012;*

- Galdieri, *Teoria e pratica dell'interpretazione del reato informatico,* Milano 1997;

- Galdieri, *"Reati informatici e responsabilità delle persone giuridiche: l'Europa chiede una riforma – Reati informatici e attività di indagine - Lo stato dell'arte e prospettive di riforma", 2006;*

- Garante per la protezione dei dati personali: *Relazione 2010. Evoluzione tecnologica e protezione dei dati*, Roma, 2011, p. 95;

- Garrie – Wong, *Privacy in Electronic communication: The regulation of Voip in the E.U. and in the U.S.A.*, in Computer and Telecommunication Law Review 2009, 139;

- Garuti, *Le intercettazioni preventive nella lotta al terrorismo internazionale,* in dir. Penale e Processo, 2005;

- Gatti - Vannini, *Persone semplici, organizzazioni complesse: un caso di phishing transazionale. L'operazione Oracolo, problematiche e suggestioni,* intervento a IISFA FORUM 2011 - Milano, 13 maggio 2011;

- Giannantonio, *L'oggetto giuridico dei reati informatici*, in Cass. pen., 2001, (7), p. 2244 ss;

- Griffo, *Limiti all'integrazione del decreto adottato ai sensi dell'art. 268 comma 3,* Cass. pen., Sez. Un., 29 novembre 2005, Campenni, in Cass. Pen. 2006, p. 1347;

- Gualtieri, *La prova scientifica*, in Diritto penale e processo, 2011, 493 e ss.

- Iacobacci, *Sulla necessità di riformare la disciplina delle intercettazioni prendendo le mosse dalle esitazioni applicative già note*, in Giust. pen., Ill, 2011, p. 365 ss

- Koester, *Voip goes the bad guy: understanding the legal impact of the use of Voip in cases of NSA warrantless eavesdropping,* in John Marshall journal of Cmputer and Information Law 2006, 227;

- Lametta, *Kriptonite, fuga dal controllo globale. Crittografia, anonimato e privacy nelle reti telematiche*, Torino 1999;

- Laronga, *Il pedinamento satellitare: un atto atipico lesivo di diritti inviolabili?* QG, 2002, 1157;

- Lisi - Murano - Nuzzolo, *I reati informatici. La Disciplina penale nella società dell'informazione. Profili procedurali*, Maggioli, 2004;

- Lorenzetto, *Le attività urgenti di investigazione informatica e telematica,* in Sistema Penale e criminalità informatica (a cura di Luparia), Milano 2009;

- Lorenzetto, *Utilizzabilità dei dati informatici incorporati sui computer in sequestro,* in Cass. Pen. 2010, 1522;

- Luparia – Ziccardi, *Investigazione penale e tecnologia informatica,* Giuffrè 2010;

- Luparia, *Sistema penale e criminalità informatica*, Milano 2009;

- Luparia, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. I profili processual*i in Dir. Penale e processo 2008, 718;

- Luparia, *Processo penale e tecnologia informatica* in Diritto dell'internet, n°3 del 2008, p. 221 ss.;

- Luparia, *Computer crimes e procedimento penale,* in Trattato di Procedura Penale diretto da Spangher, vol VII tomo I, a cura di Garuti, pp. 369 e ss.;

- Luparia, *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Giuffrè, Milano, 2012;

- Luparia, *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul cybercrime*, in S. LORUSSO (a cura di), Le nuove norme sulla sicurezza pubblica, Padova, 2008, p. 63 ss.;

- Maioli – Cugnasco, *Profili normativi e tecnici delle intercettazioni: dai sistemi analogici al voice over IP,* in Gedit edizioni, Bologna 2008;

- Manchia, *Localizzazione tramite gps, quali garanzie?* In RG Sarda, 2006, p.432;

- Manna, *Erosione delle garanzie individuali in nome dell'efficienza dell'azione di contrasto al terrorismo: la privacy*, in Riv. it. dir. proc. pen., 2004, 1022;

- Marafioti, *Digital evidence e processo penale*, Cassazione Penale, 2011;

- Marcolini, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in Cass. Penale 2010, p. 2855;

- Marinelli, *L'attività dell'agente provocatore per il contrasto alla pedo-pornografia: "straripamenti" investigativi e relative implicazioni processuali,* in Cass. Pen. 2005, 9, p.2683;

- *Marinucci -Dolcini, Manuale di diritto penale,* Milano, 2004;.

- Mariotti – Tacconi, *Riflessioni sulle problematiche investigative e di sicurezza connesse alle comunicazioni Voip,* in Diritto dell'Internet, 2008, p.558;

- Marzaduri, *Giurisprudenza sistematica di diritto processuale penale*, dir. Chiavario - Marzaduri, Torino, 1999;

- Mauro – Gargiulo, *Privacy sicurezza, data retention e sorveglianza globale: Voip security,* in Dir. Pen. e Processo 2010, p.1309;

- Mattiucci - Delfinis, *Forensic Computing*, in Rassegna dell'Arma dei Carabinieri, 2006 pp.66 e ss.;

- Melillo, *Attribuzioni processuali in tema di misure di prevenzione e di reati informatici*, Torino 2008;

- McCcullagh, *Skype: we cannnot comply with police wiretap requests* in CNET online review, 09 giugno 2008;

- McCcullagh, *FBI to announce new Net wiretapping push* in CNET online review, 16 febbraio 2011;

- Meoli – Scardaccione, *Fenomeni telematici e intercettazioni:profili giuridici e regolamentari* in Amministrazione & Finanza n.17/2003;

- Meyer D. *EU Agency backtracks on Skype crime claims,* in CNET online review, 27 febbraio 2009;

- *Microsoft - 2012 Law Enforcement Requests. Report. Principles, Policies and Practices"*

- Mitnik – Simon, *The art of Deception,* Feltrinelli 2003;

- Mitnik, *The art of intrusion,* Feltrinelli maggio 2006;

- Monsurrati – Tonacci; *I boss si parlano su Skype, adesso intercettarli è diventato impossibile,* La Repubblica, 14 febbraio 2009 pg.23;

- Monsurrati - Tonacci, *Boss ed intercettazioni: Skype sotto accusa*, in La Repubblica del 15 febbraio 2009;

- MONTI, *No ai sequestri indiscriminati di computer,* in Diritto dell'internet, 2007, (3), p. 264 ss.

- Nevoli, *Intercettazioni informatiche e telematiche: ricorso ad impianti esterni ed obbligo motivazionale del P.M.* in Arch. Nuova Proc. Pen. 1/2010,76;

- Nappi., *I dati esteriori delle conversazioni telefoniche e la loro pretesa riconducibilità al concetto di comunicazione*; in D.&G., 2000, n.8, pp.72 ss.;

- NAPPI - SARAVO, *L'approccio multidisciplinare nella gestione della scena del crimine*, in Dir. pen. proc., 2011, (5), p. 623 ss.

- Obizzi*, I reati commessi su Internet: computer crimes e cybercrimes.* Udine*, 2009;*

- L. Paccagnella, *La comunicazione al computer. Sociologia delle reti telematiche*, Il Mulino Bologna 1^ed.2000.

- Parodi, *La disciplina delle intercettazioni telematiche,* in Dir Pen. e Processo 2003, p.889;

- Parodi, *Voip, Skype e tecnologie di intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?,* in Dir. Pen. e Processo 2008, p.810;

- Parrillo – Donna, *The current status of Voip regulation in Italy*, in Computer and Telecommunication Law Review 2006, 109;

- Pecorella, *Il diritto penale dell'informatica*, Cedam Padova 2006;

- Pecorella, *L'attesa pronuncia delle sezioni unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*, in Cass. pen., 2012, (11), p. 3681 ss.;

- Peretoli, *Controllo satellitare con GPS: pedinamento o intercettazione?*,in Dir. pen. e processo, 2003, p. 94;

- Perri, *La computer forensics*, in Manuale breve di informatica giuridica, a cura di G. Ziccardi, Milano, 2006;

- Perri, *Un'introduzione alle investigazioni scientifiche,* in Ciberspazio e diritto, 2008, (2), p. 145 ss.;

- PERRI, Computer forensics (indagini informatiche), in Dig. disc. pen., Torino, Agg. 2011, p. 95 ss.

- Piga, *Diritto penale delle tecnologie informatiche*, Torino 2000;

- Piccinni - Vaciago, *Computer crimes. Casi pratici e metodologie investigative dei reati informatici*, Moretti & Vitali, 2008;

- Picotti, *Reati informatici (voce),* in Enc. giur. Treccani, agg. VIII, Roma, 2000, p. 1

- Picotti, *La nozione di "criminalità informatica"* e la sua rilevanza per le competenze penali europee, in Riv. trim. dir. pen. ec., 4, 2011, 827 e ss;

- Picotti, *Ratifica della convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo* in Dir. Internet 2008, p.437;

- Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), Il diritto penale dell'informatica nell'epoca di internet, Trento, 2004, p. 21 ss.;

- Picotti, *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici,* in Bertolino – Forti (a cura di), scritti per Federico Stella, II, Napoli, 2007,p. 1267;

- Pierro*, Introduzione allo studio dei mezzi di ricerca della prova informatica*, in Dir. pen. proc, 2011, (12), p. 1516 ss.;

- Rebecca, *Intelligence e controllo delle comunicazioni telematiche nella legislazione statunitense antiterrorismo*, in Dir. pen. proc., 2003, pp.1292 ss.

- Rafaraci, *Intercettazioni ed acquisizioni di tabulati telefonici*, in Kostoris – Orlandi (a cura di) Contrasto al terrorismo interno ed internazionale, Torino, 2006, 265;

- RESTA, Cybercrime e cooperazione internazionale, nell'ultima legge della legislatura, in
- Giur. merito, 2008, (9), p. 2147 ss.

- Ricci, *Digital evidence e irripetibilità delle operazioni acquisitive,* in Diritto pen. e processo, 2010, 339;

- Rispoli, *Le intercettazioni telefoniche, telematiche ed ambientali, e loro (in)utilizzabilità nel procedimento diverso, tra esigenze della Giustizia e diritti della persona,* in Diritto e Giustizia 2009, 171;

- Ruggeri*, Sub art. 5 d.l. 18 ottobre 2001, n. 347, conv. con mod. dalla l. 15 dicembre 2001, n. 438*, in Legisl.pen., 2002, 795.

- Salvadori, *Hacking, cracking e nuove forme di attacco ai sistemi d'informazione. Profili di diritto penale e prospettive de jure condendo*, in Ciberspazio e diritto, 2008, (3), p. 329 ss.;

- Santoriello - Dezzani, *Il reato di accesso e trattenimento "abusivi" nel sistema informatico e la responsabilità amministrativa delle persone giuridiche*, in La responsabilità amministrativa delle società e degli enti, 2012, (1), p. 57 ss.;

- Sarzana dI S. Ippolito, *L'accesso illecito alle banche dati ed ai sistemi informatici pubblici: profili giuridici*, in Il diritto dell'informazione e dell'informatica, 2007, (2), p. 277 ss.;

- Sarzana Di S. Ippolito, *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in Dir. pen. proc., 2008, (12), p. 1562 ss.;

- Sarzana, *Informatica, Internet e diritto Penale*, Milano 2010;

- Sarzana *"La criminalità informatica: aspetti processuali"* in Quaderni del C.S.M., 1994 pg 348;

- Sarzana, *Informatica e diritto penale*, Milano, 1994, 247;

- Sarzana Di S. Ippolito, *Informatica, internet e diritto penale,* Milano, 2010;

- Sbisà, *Cenni sul computer come strumento di prova nel processo penale*, in Il Foro Ambr., 2000, p. 98;

- Scaglione, *Attività atipica di polizia giudiziaria e controllo satellitare*, in Foro Italiano 2002, p.635;

- Scalco, *L'indagine Voip e P.A. – il comune di Loria "cavia" perfetta*, in e-Gov Magazine 2009, p.44;

- Scalise I, *Ingegneria sociale e sicurezza informatica,* apparso su SwZone.it del 28 aprile del 2008;

- Scognamiglio, *Criminalità informatica,* Napoli, 2008;

- Scuderi, *Un caso di hacking: luoghi reali e luoghi virtuali tra diritto e informatica*, in Ciberspazio e diritto, 2006, (7), p. 377 ss.;

- Selvaggi, *Sul sequestro operato dalla polizia giudiziaria*, in Cass. pen., 1991, (12), p. 925 ss.;

- Sieber, *La tutela penale dell'informazione*, in Riv. trim. dir. pen. ec., 1991, (2-3), p. 495 ss.;

- Signorato, *La localizzazione satellitare nel sistema degli atti investigativi*, in Rivista italiana di diritto e procedura penale, II, 2012, pp580 ss. ;

- Signorile, *Computer forensics guidelines: un approccio metodico-procedurale per l'acquisizione e l'analisi della digital evidence*, in Ciberspazio e diritto, 2009, (2), p. 197 ss.;

- Silbert – Chilton, *Gigabit by Gigabit: Technology's potential erosion of the fourth Amendment*, in Crim. Just. 2010, p.5;

- Siracusano, *Le prove*, in Siracusano – Galati -. Tranchina - .Zappalà, *Diritto processuale penale,* Milano, 2001.

- Smith G.J.H., *Internet Law and regulation*, Sweet and Mawell, 2002, pp. 347-349;

- Stalla, *L'accesso abusivo ad un sistema informatico o telematico*, Milano 2000;

- Stramaglia, *Il pedinamento satellitare: ricerca ed uso di una prova "atipica",* in Dir. pen. proc, 2011, p. 214.

  Testa, *"Cybercrime, intercettazioni telematiche e cooperzione giudiziaria in materia di attacchi ai sistemi informatici"*, "Persona e danno" del 27.02 2009;

- Tonini, *Prove scientifiche e scienza delle prove,* Giuffrè, 2012*;*

- Tonini, *Documento informatico e giusto processo*, in Dir. Pen e Processo 2009 pp. 406 e ss.;

- Tonini, *Manuale di procedura penale*, Milano, 2011;

- *Trattato di Procedura Penale* diretto da Giorgio Spangher vol.VII tomo I, UTET 2011;

- Uguccioni, *sub art. 11 L23 dicembre 1993 n.547*, in Leg. Pen., 1996, p.140;

- Vaciago, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato,* Torino, 2012;

- Vaciago, *La disciplina normativa della data retention e il ruolo degli internet service provider*, in L. LUPÀRIA (a cura di), Internet provider e responsabilità penali, Milano, 2012, p. 141 ss.

- Vaciago, *Le investigazioni telematiche,* Milano 2008;

- Vaciago, *Computer crimes. Casi pratici e metodologie investigative dei reati informatici* Bergamo 2008;

- Velani. *Nuove tecnologie e prova penale: il sistema di individuazione satellitare g.p.s.*, in Giur. it., 2003, p. 2375;

- Venturini, *Sequestro probatorio e fornitori di servizi telematici*, in Lupària (a cura di), Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale, Milano, 2012, p. 116 ss.;

- Wikipedia, *Sicurezza informatica* e voci correlate, consultazione mese ottobre 2012;

- White – Matthews - Snow - Monrose., *Phonetic reconstruction of encrypted Voip conversation,* in Security and Privacy Simposium, maggio – giugno 2011

- Zeno Zencovich, *I rapporti fra responsabilità civile e responsabilità penale nelle comunicazioni su Internet*, in Diritto dell'informazione e dell'informatica, 1999, p. 1049;

- Zeno Zencovich, Art. 8, in AA.VV., *Commentario alla Convenzione per la tutela dei diritti dell'uomo e delle libertà fondamentali*, a cura di Bartole – Raimondi – Conforti, Cedam Padova, 2001, pp.307 e ss.;

- Ziccardi, *Informatica, comportamenti e diritto: dalla computer ethics alla computer forensics,* in Ciberspazio e diritto, 2008, (4), p. 395 ss.

- ZICCARDI, *Etica e informatica,* Milano, 2009;

- Ziccardi, *Investigazione penale e tecnologia informatica,* Milano 2007;

- ZIccardi, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche,* in L. LUPÀRIA (a cura di), Sistema penale e criminalità;
- informatica, Milano, 2009, p. 165 ss

- Ziccardi, *Manuale breve di informatica giuridica*, Milano 2008;