filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Cybercrime e diritti fondamentali nell'era di Internet

09 Maggio 2017
Enrico Sericola

[Contributo selezionato da Filodiritto tra quelli ricevuti nell'ambito del concorso promosso da ELSA nel 2016 sul tema: "Internet e le nuove tecnologie"]

L'acquisizione della prova digitale nel processo penale come cristallizzata nella L.2008, n.48 e rapporti con il principio di stretta legalità di cui all'art.25 della Costituzione.

INDICE

PREMESSA

La rivoluzione tecnologica dell'ultimo ventennio ha influenzato la maggior parte delle attività umane, coinvolgendo ogni aspetto sociale e giuridico dei consociati, di tipo lavorativo, politico, privato, pubblicistico.

Alla carica innovatrice e rivoluzionaria del fenomeno Internet, certamente non sfugge la più alta forma di attività umana, che ogni cosa ricomprende, ovvero il diritto, considerato come ordinamento del sociale.

L'avvento dell'era digitale, in particolare sul piano del diritto penale sostanziale, ha determinato una trasformazione nella fisionomia delle tradizionali forme di criminalità, inducendo altresì una crescita esponenziale della frequenza con cui, grazie all'uso dello strumento informatico, sono perpetrati gli illeciti comuni.

Ma **i nodi più problematici della "rivoluzione digitale" si devono sciogliere da una prospettiva strettamente processuale e si riscontrano nel fatto che la prova, nella sub-specie documentale, finisce ormai quasi sempre nell'annidarsi in dispositivi di memorizzazione virtuale delle informazioni**.

Il *computer*, in senso lato, ha acquisito, al giorno d'oggi, una importanza sempre maggiore quale fonte probatoria rispetto a qualunque forma di processo penale, dalle indagini previste per i reati associativi legati alla criminalità organizzata a quelle previste per i casi di terrorismo internazionale, sino ai casi di omicidio, smettendo di rilevare esclusivamente quale elemento costitutivo della fattispecie o come mezzo

attraverso il quale viene realizzato l'illecito.

Tutto questo ha prodotto difficoltà di contrasto sempre maggiori in capo alle autorità investigative, in diretta correlazione con le infinite potenzialità di Internet e del *Cyberspazio*. Tali crescenti difficoltà, al fine di rimanere al passo con i tempi, hanno sollecitato gli inquirenti a **spingersi oltre le frontiere tradizionali dell'investigazione, spesso eccedendo il limite che in uno Stato di diritto è rappresentato dal rispetto delle garanzie individuali e costituzionali**.

Lo scontro tra nuove metodologie investigative e nuove forme di criminalità, all'interno del processo penale, si traduce nello sforzo continuo da parte del legislatore e degli interpreti di mediare due essenziali ma contrapposte esigenze: l'accertamento del fatto e la tutela dei diritti fondamentali degli individui coinvolti in tale accertamento.

Il *punctum dolens* è sempre lo stesso: saper trovare un giusto equilibrio tra tutela della società e rispetto dei principi fondamentali della persona (filosofeggiando con un broccardo di Orazio: «In media stat virtus!»).

A proposito di *digital evidence*, si deve porre all'attenzione dell'interprete il concreto pericolo di malleabilità della materia e della possibile alterazione delle fonti di prova, visto l'elevato grado di tecnicità che connota l'intera *sedes materiae*.

Il rischio è quello di una incontrollata introduzione di una *junk science* e di una manifesta, ingiustificata ingerenza nel diritto alla *privacy* degli individui, problematiche che richiedono estrema cautela: l'interprete è tenuto a verificare con rigore la compatibilità degli strumenti offerti dal progresso scientifico rispetto ai principi cardine del processo penale, *in primis* con l'art.25 della Costituzione Repubblicana del '48, *in secundis* con l'esigenza di garanzia del diritto di difesa, inviolabile in ogni stato e grado del procedimento.

Il sistema penale italiano, a seguito dell'entrata in vigore della legge 18 marzo 2008, n.48 di ratifica della Convenzione di Budapest sul ***cybercrime***, sembra aver acquisito una consapevolezza maggiore riguardo alla rilevanza di tale tematica, in modo da fronteggiare con disposizioni puntuali e uniformi alle discipline degli altri Paesi europei, i fenomeni emergenti di criminalità informatica.

D'altronde, come spesso accade, tutti i tentativi finora portati avanti, si sono rivelati appena sufficienti e non esaustivi, deludendo quelle che erano le più rosee aspettative di molti.

È evidente che la scelta del legislatore di conferire un così ampio spazio di discrezionalità al giudice nella regolamentazione di una materia così complessa e delicata, è opinabile e soggetta a critiche, in quanto incauta, per non dire azzardata. Tra i più autorevoli, c'è chi auspica, quindi, nuovi interventi del legislatore, nella speranza che tale *impasse* possa risolversi rapidamente; cosa più che condivisibile, del resto, se il rispetto dei principi costituzionali rimane il *primum movens* da salvaguardare.

PARTE PRIMA

L'avanzare della legislazione contro il *Cybercrime*.

Dall'inizio degli anni '90, il combinato disposto tra l'evoluzione degli strumenti comunicativi e lo sviluppo delle nuove tecnologie, ha indotto il legislatore alla introduzione dei *computer crimes* nel catalogo degli illeciti racchiusi nella parte speciale del libro secondo del codice penale ed all'inserimento nel sistema di una prima forma di raccolta della prova digitale, la cosiddetta "captazione informatica".

L’approccio tra informatica e reti telematiche ha originato ampie possibilità di sviluppo per la società attraverso attività di *e-commerce*, di *home-banking*, di *trading on line*, rendendola nel contempo estremamente *net-centrica*[1] e ha consentito, dunque, ad una serie di attività illecite (i c.d. reati informatici) di sfruttarne l’evoluzione.

L’espansione del *cybercrime* può considerarsi come un prodotto logicamente consequenziale alla inarrestabile ascesa del fenomeno Internet nel mondo che, se da un lato, ha offerto molteplici opportunità sul piano sociale, culturale ed economico, dall’altro ha fornito un *humus* fertile per l’affermarsi di comportamenti *contra legem* da parte dei suoi stessi fruitori. Alla criminalità informatica non viene assegnata una categoria giuridica *ad hoc*, nonostante compaia in numerose fonti europee e sovranazionali[2].

Come, del resto, non si rinviene una definizione unanime, internazionalmente riconosciuta di “*computer crime*” o “*cyber crime*” proprio a causa della varietà delle condotte che possono essere compiute attraverso il *cyberspazio*. Sotto un profilo di carattere penale sostanziale, in riferimento alla criminalità informatica, si possono tipicizzare, fondamentalmente, due fattispecie di condotte legate a modalità, oggetti o attività di carattere tecnologico ovvero a fattispecie incriminatrici comuni che possono vedersi configurare attraverso la rete o nel *cyberspace*[3].

La prima vera normativa contro l’emergente fenomeno del *cybercrime* nel nostro ordinamento è stata la **legge 23 settembre 1993, n.547** (*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*) che, oltre ad aver novellato il codice penale attraverso la disciplina dei reati informatici, ha previsto anche uno specifico mezzo di ricerca della prova, vale a dire le intercettazioni del flusso di comunicazioni relativo a sistemi informatici (telematici), ovvero intercorrente fra più sistemi.

Successivamente le leggi 18 marzo 1978, n.191 (che ha introdotto l’art.420 c.p., contro l’attentato ad impianti di elaborazioni dati) e 1 aprile 1981, n.121 (a garanzia e tutela dei dati archiviati in un sistema informatico), ma bisognerà attendere un decennio per normative più specifiche al garantismo di una maggiore tutela in ambito informatico, come la legge 5 luglio 1991, n.197 (sull’antiriciclaggio di denaro) o il d.lgs. 29 dicembre 1992, n.518 inerente ai reati di “pirateria informatica”.

Il periodo precedente all’approvazione della legge n.547 del 1993, aveva visto dottrina e giurisprudenza impegnate nel ricondurre le nuove figure criminose a fattispecie tradizionali.

Nessun problema, in effetti, si poneva riguardo alla parte fisica (*hardware*) del sistema informatico, che poteva essere agilmente ricondotta alle figure delittuose tradizionali, quali danneggiamento, furto ecc.; **per quanto concerne, invece, i delitti commessi sul complesso dei dati e delle informazioni che costituiscono la parte logica (*software*) del sistema informatico, in questi specifici casi si è posto il problema dell’identificazione della condotta criminogena**.

A titolo di esempio, l’alterazione del funzionamento di un *software* che consente un indebito accredito di ingenti somme di danaro, provoca sicuramente una condotta illecita assimilabile alla fattispecie di truffa ex art.640; tuttavia la mancanza degli elementi necessari del reato, quali gli “artifizi e i raggiri”, non ha consentito una corretta applicazione del delitto di truffa ed è andata a configurare, nel caso di specie, un emblematico caso di analogia *in malam partem*[4].

La legge 547 del 1993 ha ristabilito, pertanto, la validità del celebre brocardo “*nullum crimen, nulla poena sine praevia lege poenali*”, colmando una lacuna protrattasi per troppi anni, e rispondendo, allo stesso tempo, a quella serie di istanze sovranazionali orientate verso la realizzazione di una disciplina uniforme tra le varie nazioni, conformandosi, parallelamente, tutti gli Stati su di una direttrice univoca:

collaborazione e lotta penale altamente repressiva delle nuove figure delittuose.
Antecedentemente alla sottoscrizione della Convenzione di Budapest sul *cybercrime* e alla sua conseguente ricezione con la legge 18 marzo, n.48 la scena investigativa e processuale all'interno del nostro ordinamento era contraddistinta da prassi ed indirizzi giurisprudenziali oscillanti ed altalenanti. **Numerosi sono i casi, infatti, in cui la discrezionalità garantita al giudice nella valutazione ed acquisizione delle prove è stata privilegiata rispetto ad un'analisi ossequiosa degli *standards* , delle procedure, dei parametri, dei principi nonché delle acquisizioni teoriche della *computer forensics* (o generalmente della *digital forensics*)**[5].
Si pensi, ad esempio, ai casi di valutazione processuale dei *file log* e di altri dati, relativi al numero IP assegnato all'utente, all'individuazione dell'identità dell'utente, ai tempi di connessione, all'individuazione delle pagine visitate e dei loro contenuti, forniti dagli *Internet Service Providers* (ISP), **a richiesta dell'autorità e senza l'autorizzazione né di specifici controlli né di contraddittori con l'indagato**[6].
La **legge di ratifica della Convenzione di Budapest del 23 novembre 2001** ha introdotto nel codice di procedura penale una serie di disposizioni normative atte a regolamentare istituti già esistenti nel codice di rito (come quello delle ispezioni o delle perquisizioni o dei sequestri) ma aggiornati rispetto a quella necessità di operare secondo determinati standard di *computer forensics*.
L'ondata innovatrice della riforma ha portato con sé come conseguenza modifiche significative di diverse norme del codice di procedura penale. In particolare, le disposizioni che hanno subito una modificazione rilevante sono state: l'art.244, comma 2, c.p.p., in tema di ispezioni, gli artt.247, comma 1-bis e 248, comma 2 c.p.p. in materia di perquisizioni, l'artt.254 e 254-*bis* c.p.p. in tema di sequestri[7].

PARTE SECONDA

Computer Forensics e digital evidence nelle indagini penali.
La *computer forensics* (o *digital forensics*), intesa come "*the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media*»[8] è la disciplina, dunque, che focalizza la sua attenzione sulle informazioni ed i dati conservati o elaborati dalle apparecchiature digitali senza avere la presunzione di circoscrivere il novero degli esempi prospettabili in tal senso.
Pertanto, **non è ipotizzabile un'unica *best practice* a livello normativo e una canonizzazione della materia rischierebbe di rendersi inopportuna ed obsoleta**.
Si è parlato, spesso, di *digital forensics*, proprio con riferimento a quella parte della scienza che si occupa della individuazione, acquisizione, analisi ed interpretazione del dato digitale al fine di evidenziare l'esistenza di indizi o fonti di prova nello svolgimento dell'attività investigativa e peritale.
La definizione elaborata dallo *Scientific Group on Digital Evidence* (SWGDE) sembra quella più esaustiva tra quelle adottate a livello internazionale; per cui **costituisce *digital evidence* "qualsiasi informazione, con valore probatorio, che sia o meno memorizzata o trasmessa in un dato digitale" e quella della *International Organization on Computer Evidence* (IOCE)**[9].
All'interno della generica categoria della *digital evidence*, si distinguono solitamente la c.d. "*computer-generated evidence*" e la c.d. "*computer-derived evidence*". Nella *computer generated-evidence* lo strumento informatico costituisce l'oggetto dell'attività probatoria: l'elaboratore, in tali casi, viene convenzionalmente utilizzato per la ricostruzione virtuale dei vari accadimenti fattuali attraverso l'analisi e l'elaborazione, con specifici *software*, dei dati inseriti al suo interno.
Nella *computer-derived evidence*, invece, si fa capo alle ipotesi in cui il dato digitale estrapolato dall'elaboratore costituisce prova diretta o indiretta di un elemento costitutivo della *res iudicanda*

.

In entrambi i casi è evidente la portata cognitiva dello strumento digitale all'interno del processo penale, ciononostante le operazioni di individuazione, acquisizione ed analisi dei dati digitali dovranno rigorosamente rispettare delle *guidelines* del sistema già in una fase precedente la loro stessa introduzione in sede dibattimentale, sia se le si voglia inserire nel novero degli **accertamenti urgenti** ex art.354 comma 2 c.p.p., sia se si decida di optare, come rilevato da autorevole dottrina, per la disciplina **degli accertamenti tecnici non ripetibili** ex artt.359 e 360 c.p.p. al fine di garantire il diritto di difesa e, soprattutto, di assicurare il contraddittorio fin dalla prima fase di trattamento del dato digitale.

Inoltre, **in merito alla presumibile illegittimità della duplicazione integrale dell'intero *hard disk* fatto oggetto di sequestro probatorio**, potrebbero sollevarsi ulteriori interrogativi. Infatti, con tale *modus operandi*, vi è la concreta possibilità di apprensione di dati ed informazioni non pertinenti all'ipotesi di reato e suscettibili di rientrare nell'ambito di tutela accordata ai diritti fondamentali della persona, quali il diritto alla protezione dei dati personali ed alla riservatezza, ovvero al diritto dell'imputato di essere messo a confronto con il dato informatico nel suo aspetto genuino, senza alterazioni[10].

Il legislatore nazionale ha introdotto rilevanti modifiche in merito all'acquisizione della prova digitale solamente nel 2008, attraverso la legge di ratifica della Convenzione di Budapest sul *cybercrime* del 23 novembre 2001, introducendo ben **cinque fasi dell'investigazione digitale (individuazione, acquisizione, conservazione, analisi e presentazione) per il valido inserimento della *digital evidence* all'interno del processo penale**. Ciò al fine di tutelare quelle garanzie di riservatezza e di difesa dell'imputato che potrebbero venir meno in seguito ad una incondizionata ed indiscriminata acquisizione probatoria non sorretta da parametri predefiniti.

Le nuove tecnologie informatiche hanno posto alla ribalta l'esigenza della "certezza delle regole" e di una corretta analisi del linguaggio criptico; è evidente che riuscire a decifrare un tabulato, interpretare un *file log*, ragionare su codici *hash*, sulle attività di *download*, sulla partizione dell'*hard disk* o sul *peer to peer*[11] non è compito agevole.

Normalmente, **il settore che si occupa dell'applicazione di metodologie tecnico-scientifiche di analisi dei sistemi operativi e degli stessi file, al fine di raccogliere prove utilizzabili in fase dibattimentale, è quello della "informatica forense"**.

La diffusione di reati di natura tecnologica, ai danni di società fortemente permeate dalla tecnologia informatica, ha avuto come conseguenza immediata la nascita di figure professionali in grado di analizzare i "sistemi vittime" e suggerire possibili soluzioni dinnanzi a tali aggressioni[12]. Scopo dell'informatica forense, infatti, ai fini della piena validità della prova e della sua utilizzabilità in giudizio, è proprio la **verificabilità delle procedure attuate durante l'intera attività investigativa, ponendosi la trasparenza delle operazioni compiute e la loro ripetibilità innanzi al magistrato giudicante, come "*conditio sine qua non*" per ogni interpretazione o perizia in materia di investigazioni informatiche**.

Illuminante il valore probatorio dato alla prova informatica da alcuni illustri autori, secondo i quali costituirebbe "*capacità di convincimento del giudice, delle parti processuali o di altri soggetti in odine alla genuinità, non ripudiabilità, imputabilità ed integrità del dato e dei fatti dallo stesso dimostrati*".

Accanto al tema affrontato sull'accertamento, l'acquisizione, l'analisi e la raccolta di materiale informatico, in tema *digital evidence*, appare necessario, come nesso logico-consequenziale, proseguire l'*iter* narrativo accennando ai problemi connessi alla legislazione in materia di privacy, nella sub-specie, in tema di *data detention*.

Nel nostro Paese la normativa sulla raccolta e l'utilizzo delle informazioni relative al traffico telefonico ed

informatico è contenuta nel decreto legislativo 30 giugno 2003, n.196, intitolato "Codice in materia di protezione dei dati personali", noto anche come Testo Unico sulla privacy, il quale, nel corso degli anni, è stato novellato più volte, da un lato per far fronte all'evoluzione dei mezzi e del mondo tecnologico, dall'altro per garantire un'effettiva tutela a nuovi diritti che man mano si sono generati.

È stato necessario attendere il d.lgs. n.109 del 30 maggio 2008, di attuazione della direttiva 2006/24/CE (c.d. direttiva Frantini) sulla conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, per avere un chiarimento, seppur generico, in tale *sedes materiae*.

Ad oggi, a norma dell'art.132 del Codice della Privacy sulla conservazione di dati di traffico per finalità di accertamento e repressione dei reati, è previsto che:

1) i dati relativi al traffico telefonico siano conservati per 24 mesi dalla data di comunicazione;

2) i dati relativi al traffico telematico siano conservati per 12 mesi dalla comunicazione;

3) i dati relativi alle chiamate senza risposta siano conservati per 30 giorni dalla data di comunicazione.

Attualmente l'intera disciplina della conservazione dei dati deve essere letta avendo riguardo ad una recente pronuncia della Corte di Giustizia dell'Unione Europea che ha invalidato la direttiva 2006/24/CE.

A detta della Corte, infatti, le prescrizioni della normativa in questione rappresenterebbero "*un'ingerenza di vasta portata e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale, non limitata allo stretto necessario*"[13].

In primo luogo la direttiva trova dunque un applicazione indiscriminata all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza operare alcuna differenziazione, limitazione o eccezione in ragione dell'obiettivo fondamentale della lotta contro i reati gravi.

In secondo luogo, si legge nella statuizione della Corte, essa non prevede alcun criterio oggettivo, contrappeso, che legittimi un accesso ai dati da parte delle autorità nazionali competenti per il solo ed esclusivo fine di accertamento e perseguimento di reati, talmente gravi, da poter giustificare le ingerenze stesse.

Posto che la sentenza della Corte di Giustizia rappresenti una vera e propria "pietra miliare" nella storia delle Comunità Europea, è da attendere ora il comportamento degli Stati membri, determinante **nella prospettiva di una normativa europea unitaria ed uniforme, ma ancor di più, per veder rispettato il principio di tassatività e di certezza del diritto, canoni su cui posano e da cui traggono linfa vitale tutte le legislazioni**.

PARTE TERZA

Intercettazioni informatico-telematiche e garanzie costituzionali.

In Italia l'utilizzo delle intercettazioni come mezzi strumentali alla ricerca di materiale probatorio nella fase delle indagini, è oramai concepito come una costante, un presupposto costitutivo ed essenziale del processo penale stesso.

Le particolari difficoltà nel maneggiare il mezzo informatico, vanno correlate ad una serie *di garanzie predisposte a livello costituzionale (e sovranazionale*[14]*) sancite proprio per evitare un depauperamento inaccettabile di quei diritti definiti "inviolabili" e, dunque, non suscettibili di limitazione alcuna se non nei limiti prestabiliti dalla Costituzione stessa*[15].

L'art.15 della Costituzione così recita: "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge". Si pone, quindi, a presidio delle stesse una ***doppia riserva di legge e di giurisdizione applicabile ogniqualvolta la comunicazione intervenga fra persone determinate, sia in forma epistolare che telefonica che telegrafica*** *(nonché tecnologica,*

dovendosi ritenere ineluttabile l'applicazione della norma costituzionale anche ai più evoluti mezzi di comunicazione tecnologici).

In base al combinato disposto dell'art.15 suddetto con l'art.2 Cost., il diritto è sancito inviolabile nel senso che ***non può subire alcuna restrizione se non in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario, altresì costituzionalmente rilevante e sempreché sia rispettata la duplice garanzia della riserva assoluta di legge e dell'atto motivato dell'autorità giudiziaria****.*

Presupposte le dovute garanzie costituzionali, nel porre rimedio al silenzio del legislatore, la giurisprudenza ha precisato che "l'intercettazione rituale consiste nell'apprensione occulta, in tempo reale, del contenuto di una conversazione o comunicazione in corso tra due o più persone da parte di altri soggetti, estranei al colloquio"[16].

In una recente pronuncia della Corte EDU (Donato d'Auria e Balsamo c. Italia, decisione dell'11 giugno 2013 n.11625/07) sono state confermate le linee argomentative, in tema di intercettazioni, maturate dalla giurisprudenza nazionale recentemente.

La Corte, nella fattispecie, sottolinea che rientrando le comunicazioni telefoniche nella nozione di "vita privata" ai sensi dell'art.8 della Convenzione[17]*, la loro intercettazione e memorizzazione dei dati così ottenuti ed il loro eventuale utilizzo nell'ambito dei procedimenti penali costituisce una ingerenza da parte dell'autorità pubblica nel godimento di un diritto;* ***tale ingerenza può essere legittima solo se giustificata e tassativamente disciplinata*** *(in base al secondo comma dell'art.8, nei casi di sicurezza nazionale, benessere economico dello Stato, prevenzione dei reati, protezione della salute o della morale, protezione dei diritti o delle libertà altrui).*

In caso contrario, il rischio inevitabile è quello di minare o addirittura distruggere la democrazia che si presume di difendere.

Oggigiorno non esiste cosa più semplice del comunicare e diffondere informazioni in maniera economica ed immediata. E questo grazie alla grande varietà di dispositivi e mezzi di comunicazione che le nuove tecnologie hanno offerto negli anni, tanto da far ribattezzare il nostro secolo come il "secolo dell'informazione".

Sicuramente la comunicazione telematica è stata di gran lunga quella più incisiva nei rapporti interpersonali data la capacità da parte di qualsiasi elaboratore elettronico, fornito di una connessione a banda larga, di porsi come strumento di comunicazione polifunzionale. Ma se da un lato questo tipo di soluzione ha consentito di abbattere ogni barriera, favorendo una comunicazione "senza frontiere", dall'altro si è offerta un'occasione d'oro agli "esperti del crimine" per la realizzazione di illeciti sempre più sofisticati ed al passo con la tecnologia (si pensi ai c.d. *cybercrimes*).

A fronte di queste preoccupazioni, il legislatore, con la legge 23 dicembre 1993 n.547, ha introdotto nel codice di procedura penale l'art. 266-*bis* c.p.p. volto alla regolazione delle "**Intercettazioni Telematiche**".

L'art.266-*bis* c.p.p., nella sua interpretazione più ampia ed in linea con lo spirito del riformatore, ha dunque consentito la captazione del contenuto di *mail* inviate e ricevute, dei siti *web* visitati, di conversazioni in chat room, di *download* ed *upload* di *files* nonché delle comunicazioni VoIP non criptate. Ogni comunicazione elettronica, infatti, può essere oggetto di intercettazione allo scopo di acquisire, modificare, copiare i dati in essa contenuti sfruttando i punti maggiormente vulnerabili del "sistema" quali router, le gateway o i server di rete.

L’ecletticità delle metodologie di comunicazione ha obbligato gli organi inquirenti ad una maggior presa di consapevolezza dei cambiamenti in atto, ai fini di una maggior tutela del livello di riservatezza di ogni singolo cittadino.

Le intercettazione, laddove disposte, potranno avvenire con svariate modalità, condizionate da alcuni elementi*: innanzitutto si dovrà accertare il tipo di connessione utilizzata dall’utente (come ADSL o analogica) ma soprattutto conoscere tecnicamente il “service provider” utilizzato. Il provider, infatti ha il compito di registrare i log relativi alla connessione di rete effettuata da ciascun utente che abbia username e password registrati.*

I cosiddetti ***file di log****[18] sono, pertanto, i dati relativi a ciascuna connessione effettuata per il tramite di quel provider, ed in particolare* ***consentono di individuare da quale utenza viene effettuata la connessione, la sua durata ed i siti visitati****.*

Nello specifico, l’intercettazione può avvenire tramite la canalizzazione del traffico di rete presso l’I.S.P. [19], attraverso una sonda detta Front End collegata ad una porta (mirror) ricevente in copia tutto il traffico scambiato, in entrambe le direzioni, dall’apparato di accesso che gestisce la connessione finale dell’utente. Il flusso dei dati sarà poi trasmesso tramite linea dedicata ad alta velocità (RES) verso la postazione di decodifica della P.G. (Back End).

Un esempio di questa forma di collaborazione con il service provider avviene nel caso dell’intercettazione della corrispondenza elettronica: ***il gestore del servizio, una volta ricevuta la “griglia” (un documento identificativo di dati tecnici consegnato dall’Autorità Giudiziaria alla Polizia Giudiziaria contestualmente al decreto autorizzativo delle intercettazioni), provvederà alla duplicazione della casella di posta elettronica dell’indagato, inoltrando tutte le e-mail direttamente al server della Procura della Repubblica****.*

Un ulteriore questione assai rilevante e capace di catturare l’attenzione dei più illustri giuristi di informatica forense ed i più esperti tecnici del settore, è stata quella attinente alle intercettazioni di comunicazioni realizzate attraverso l’impiego di apparati mobili collegate a WI-FI “aperte” o effettuate da utilizzatori di sistemi crittografati. È evidente che in questi casi un modello “classico” diretto all’acquisizione dei soli dati che fluiscano lungo la rete “in chiaro” è del tutto inefficiente. Per questo motivo sono stati creati nuovi modelli, meccanismi per l’acquisizione per queste particolari species di intercettazioni: il programma “trojan horse”, ossia un software che, prescindendo dalle autorizzazioni dell’utente, si installa e si esegue su un sistema target (sia esso un personal computer o smartphone) e ne acquisisce determinati poteri di gestione[20]. Una vera e propria microspia telematica.

La legittimazione procedurale all’utilizzo degli strumenti investigativi in questione è derivata, nella casistica, dall’applicazione dell’art.266-bis c.p.p, sotto forma di estensione delle modalità tecniche di captazione delle comunicazioni telematiche, vista l’assenza di una procedura ad hoc.

Appare evidente, pertanto, come questo profilo meriti approfondimenti ancor più precisi, da parte della dottrina e della giurisprudenza, per suggerire al legislatore degli accorgimenti puntuali, onde evitare una compressione esponenziale delle libertà fondamentali che tali sistemi possono compromettere, pur in assenza di una normativa specifica che ne disciplini i connotati essenziali.

CONCLUSIONI

Giunti al termine di questo breve contributo sul mondo informatico applicato al diritto, sembra opportuno constatare che ogni testo, ogni articolo giuridico, ogni manuale, nel definire il concetto di prova digitale e delle relative correlazioni processuali, ha presupposto sempre la sua immaterialità e categorizzato quale

elemento fluido e di difficile apprensione.

Che il dato digitale sia fortemente **vulnerabile** è dato intuibile ed oggettivo; non sarebbe stata recepita, altrimenti, una Convenzione ad *hoc* per predisporre le cautele necessarie. Ma fino a che punto una prova così "malleabile" può coniugarsi con il requisito "dell'oltre ogni ragionevole dubbio" in sede di condanna?

È evidente che la fragilità del dato informatico non può essere motivo per escludere *ex ante* la rilevanza della prova, onde evitare di escludere mezzi probatori che potrebbero rilevarsi essenziali per la formazione di una "giusta" condanna. Al contrario se ne potrebbero esaltare gli straordinari aspetti positivi di certezza ed affidabilità, rispettando così il principio cardine dell'intero ordinamento penale, ovvero il principio di stretta di legalità, costituzionalmente sancito nell'art.25 della Costituzione.

Ci si trova, dunque, davanti ad una scelta alternativa: o si accetta e condivide l'ipotesi di poter usufruire di una dato immateriale e facilmente manovrabile (con "dolo eventuale" e la consapevolezza di andar ad intaccare diritti fondamentali come quello alla *privacy*) affidandosi alla esclusiva precisione delle modalità di acquisizione dello stesso, oppure si nega a tutti gli effetti una sua utilizzabilità in sede processuale, in quanto inidoneo ad assicurare la certezza dei fatti per i quali si procede violando, di fatto, la norma costituzionale.

La giurisprudenza, nel corso degli anni, ha ritenuto di non dover escludere la *digital evidence* dal novero delle prove acquisibili al processo. Forte delle innovazioni legislative intervenute in materia, ne ha **legittimato la diffusione anche in sede di indagini**, senza risolvere, però, quei contrasti che era logico sorgessero in un sistema permeato da un marcato garantismo.

In tutti i casi, infatti, **la priorità resta quella di assicurare alla persona sottoposta alle indagini le maggiori tutele, in ossequio a quel principio di presunzione di non colpevolezza sancito dall'art.27 della Costituzione**.

Dove collocare, dunque, quelle attività svolte sempre più frequentemente, non disciplinate nel codice, ma indispensabili per l'acquisizione di quanto più materiale probatorio possibile da parte del P.M?

Molteplici dubbi possono configurarsi in merito ad operazioni non regolamentate dalla legge e lesive di interessi costituzionalmente protetti; oppure sulla tollerabilità della compressione dei diritti fondamentali, a fronte di un'azione investigativa, al confine con la liceità, solo in ragione di presunzioni e di pretese punitive verosimili.

Spesso i paletti imposti dall'ordinamento sono stati aggirati attraverso il ricorso a stratagemmi normativi "di convenienza" atti a tamponare le lacune ed i vuoti lasciati dal legislatore, pur nella consapevolezza di una loro evidente inidoneità o inammissibilità processuale.

Eppure, ce lo insegnano i latini, *adducere inconvenveniens non est solvere argumentum*. In caso contrario si spianerebbe la strada ad interpretazioni estensive, late, latissime, delle norme processuali, volte a sfociare inevitabilmente in derive giurisprudenziali tendenziose.

L'auspicio è quello di un intervento deciso e concreto del legislatore che, sulla scia di quanto realizzato a seguito della ratifica della Convenzione di Budapest sul Cybercrime, rafforzi gli apparati normativi esistenti e faccia propri quegli insegnamenti della giurisprudenza favorevoli ad una tutela preminente dei diritti della persona, ben nota alle Corti nazionali estere ed alla stessa Corte Cedu.

BIBLIOGRAFIA

BONOMO, A., *"I nuovi strumenti di comunicazione telematica ed informatica: aspetti tecnici e questioni giuridiche"*, Roma, 2011.

CAMON, A., "*Le intercettazioni nel processo penale*", Milano, 1996.
CASEY, E., "*Digital Evidence and Computer Crime. Forensics science, computers and Internet, Second Edition, Elsevier Academic Press*", 2004.
COSTABILE, G., "*Computer forensics e informatica investigativa alla luce della Legge n.48 del 2008*", in Cyberspazio e diritto, 2010.
FLOR, R., "*Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet*", in Diritto Penale Contemporaneo, 2010, pag.4.
GREVI, V., "Appunti in tema di intercettazioni telefoniche operate dalla polizia giudiziaria", in riv. it. dir. proc. pen., 1967, pag.724.
GHILARDINI, A. – FAGGIOLI, G. "*Computer Forensics*", Milano, Apogeo, 2007.
ILLUMINATI, G., "*La disciplina processuale delle intecettazioni*", Milano, 1983.
LUPARIA, L. – ZICCARDI G., "*Investigazione penale e tecnologica informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*", Milano, 2007.
MONTI, A., "*No ai sequestri indiscriminati di computer*", in Diritto dell'Internet, 2007.
ORLANDI, R., "*Questioni attuali in tema di processo penale e informatica*", in Riv. Dir. Proc, 2009.
PECORELLA, C., "*Diritto penale dell'informatica*", Padova, 2006.
SARZANA, C., "*La criminalità informatica: aspetti processuali*" in Quaderni del C.S.M., 1944, pag. 348.
TESTAGUZZA, A., "*Digital forensics. Informatica giuridica e processo penale*", Milano, 2014.
TONINI, P., "*Documento informatico e giusto processo*", in Diritto Penale e Processo, 2009.
TONINI, P., "*La prova penale*", Padova, 2000.
VACIAGO, G. "Digital Evidence, I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato", Torino, 2012.

[1] Secondo la stessa OCSE, l'utilizzo sfrenato della rete da parte di un'utenza scarsamente alfabetizzata aumenta i rischi e i pericoli su cui è possibile imbattersi ed è, probabilmente, una delle cause principali della diffusione su ampia scala del *cybercrime*, soprattutto in particolari categorie di illeciti. Sul punto si possono consultare le *Linee guide* dell'OCSE sulla sicurezza dei sistemi e delle reti di informazione.
[2] In primo luogo la Convenzione sul *cybercrime* adottata a Budapest il 23 novembre 2001, ma anche la direttiva 2001/29/CE in materia di protezione dei diritti d'autore, la direttiva 95/46/CE sulla tutela dei dati personali, la direttiva 2000/31/CE sul commercio elettronico e altre.
[3] FLOR, R., "*Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet*", in Diritto Penale Contemporaneo, 2010, p.4.
[4] Nella giurisprudenza di merito non sono mancati orientamenti riconducibili all'esempio suddetto. L'art.640 c.p. è stato ritenuto applicabile in una sentenza in un caso riguardante l'immissione nell'elaboratore elettronico dell'I.N.P.S. (Trib. Roma, 20 giugno 1984).
[5] Fu anche il caso "Vierika", in seguito alla decisione del Tribunale di Bologna (luglio 2005, C.S., sent. n. 1823), di considerare esaustive le risultanze probatorie acquisite durante la fase delle indagini, in relazione al *software* in esame, senza ravvisare la necessità di accertamenti peritali, così richiesti dalla difesa sin dalla fase predibattimentale. La mancata predisposizione degli stessi venne, in seguito, posta a fondamento dei motivi di appello della sentenza di condanna in quanto il percorso motivazionale della pronuncia fu ritenuto viziato da una ricostruzione tecnico-informatica priva di fondamento.

[6] Sul punto BRAVO, F. "*Indagini informatiche e acquisizione della prova nel processo penale*" in Rivista Criminologica, Vittimologia e Sicurezza, Vol. III, settembre 2009, p.235.

[8] L'art.244, comma 2 c.p.p., è stato novellato nel senso che sono state aggiunte le seguenti parole: «anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

All'art.248, comma 2 c.p.p., modificate ad «atti, documenti e corrispondenza presso banche» le parole: «nonché dati, informazioni e programmi informatici».

Dopo l'art.254 del c.p.p. è stato inserito l'art.254-*bis* (Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni).

[9] NOBLETT, M.G., POLLITT, M.M., PRESLEY, L.A., *Recovering and Examining Computer Forensics Evidence* «*Forensics Science Communications*», Vol.2.No.4,2000.

[10] Secondo la quale la *electronic evidence* va concepita come una "informazione generata, memorizzata e trasmessa attraverso un supporto informatico che può avere valore in tribunale".

[11] Il Tribunale di Pescara (sentenza del 3 novembre 26, n.1369) ha statuito che le riproduzioni a stampa, ancorché effettuate da ufficiali di polizia giudiziaria, sono da considerarsi di scarsa valenza probatoria laddove acquisite senza il rispetto delle regole tecniche dettate dall'AIPA (ora CNIPA).

[12] La denominazione *peer to peer* nasce dal fatto che la comunicazione avviene tra *host* in modalità "punto a punto" senza dover utilizzare i servizi e l'intermediazione di un *server*. Il funzionamento del servizio è il seguente: un utente vi accede e cerca un certo *file* fra tutti i soggetti connessi in un dato momento. Una vota individuato, può attivare l'opzione di *download* e prelevare il *file* immediatamente (o in un momento prefissato della giornata), attraverso una comunicazione diretta fra i due sistemi. Non intervenendo alcun *server*, questa tecnica è spesso utilizzata per trasferimenti di dubbia liceità come quelli aventi ad oggetto, per esempio, filmati o brani musicali coperti dal diritto d'autore o materiale pornografico. I *software peer to peer* sono progettati di solito per garantire l'anonimato dell'interlocutore, di cui si potrà conoscere eventualmente solo il *nickname*. Non sarà conoscibile pertanto l'indirizzo IP utilizzato dal computer in cui si consente l'accesso ai dati o da cui prelevano i *files* se non per il tramite di appositi *software* (o *virus*), impiegabili da tecnici specializzati.

[13] Un recente caso, famoso alle cronache giudiziarie (il caso "Stasi"), può chiarire quanto il corretto uso delle *best practice* nel "maneggiare" una prova digitale possa essere fondamentale e risolutivo. Nella sentenza n. 10491 del 5 marzo 2014, la Corte di Cassazione ha annullato senza rinvio la condanna per il delitto di detenzione di materiale pedopornografico ex art.600-quarte c.p., rinvenuto dai periti nel computer ed in un *hard disk* esterno in uso all'imputato, grazie all'utilizzo degli strumenti della *computer forensics*, attraverso i quali si è giunti a conclusioni certe e non oscillanti e tali da reggere un intero impianto accusatorio.

[14] FLOR, R., "*La Corte di giustizia considera la direttiva europea 2006/24/CE sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*", in Diritto penale contemporaneo, 28 aprile 2013, pag.3.

[15] *Pro examplo*: la "Dichiarazione Universale dei Diritti dell'Uomo" del 1948; la "Convenzione Europea sui Diritti dell'Uomo" del 1950; il "Patto sui diritti civili e politici" adottato dall'ONU nel 1966; la "Carta dei diritti fondamentali dell'UE" o meglio nota "Carta di Nizza" del 2000.

[16] Già durante l'Assemblea Costituente si osservò che: "nel momento stesso in cui il cittadino apprende l'importanza della garanzia della propria libertà e segretezza di corrispondenza e di ogni altra forma di comunicazione, la stessa non dura che un attimo seppur da che mondo e mondo, ogni e qualsiasi

Costituzione, dopo l'affermazione dei diritti fondamentali di libertà è seguita dall'enunciazione dei casi che possono limitarla", in *Atti dell'Assemblea Costituente,* seduta del 26 marzo 1947.

[17] Cfr. Corte Cost. 11 marzo 1993, n.81.

[18] Il riferimento è alla Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali del 1950 che nella prima parte dell'art.8 prevede: "*Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza*".

[19] Infatti i *files* di *log* che crea ogni *server* di accesso alla reta al momento della connessione contengono una serie di informazioni al loro interno, essenziali ai fini investigativi. Tali sono: *user name,* data e ora precisa dell'inizio e della fine della connessione (*logout*), I.P. dinamico assegnato dall' I.S.P. al momento dell'avvio della connessione alla rete e il cosiddetto callar ID, cioè numero del telefono chiamante.

[20] Acronimo di *Internet Service Provider*: struttura commerciale che offre agli utenti, dietro la stipulazione di un contratto di fornitura, servizi inerenti l'utilizzo di *Internet*.

[21] Programmi del genere sono sviluppati da aziende specializzate e sono, dal punto di vista tecnico, equivalenti a *malware* impiegati dai cybercriminali per carpire preziosi dati delle vittime.

TAG: *cybercrime, digital evidence, Informatica giuridica e diritto dell’informatica, privacy informatica, costituzionale, Diritto dell'informatica, Procedura penale*