UNIVERSITÀ
DEGLI STUDI
FIRENZE

DOTTORATO DI RICERCA IN

SCIENZE GIURIDICHE

CICLO XXVIII

COORDINATORE Prof.ssa Vittoria Barsotti

INDAGINI INFORMATICHE E PROCESSO PENALE

Indirizzo: discipline penalistiche: diritto e procedura penale

Referente di indirizzo: prof. Paolo Tonini

Settore Scientifico Disciplinare: IUS/16

Dottorando

Dott. Marco Torre

_____

Tutor

Prof. Paolo Tonini

_____

Coordinatore

Prof.ssa Vittoria Barsotti

_____

Anni 2012/2015

PREFAZIONE

PARTE PRIMA

INDAGINI INFORMATICHE CONOSCIBILI:

LA PROVA DIGITALE *OFF LINE*

CAPITOLO 1
PROVA INFORMATICA E PROCESSO PENALE

CAPITOLO 2
ISPEZIONI, PERQUISIZIONI, SEQUESTRI, RILIEVI E ACCERTAMENTI TECNICI SU MATERIALE DIGITALE

PARTE SECONDA

INDAGINI INFORMATICHE OCCULTE:

LA PROVA DIGITALE *ON LINE*

CAPITOLO 3
IL CAPTATORE INFORMATICO

CAPITOLO 4
LE INTERCETTAZIONI TELEMATICHE

CAPITOLO 5
IL PEDINAMENTO ELETTRONICO

CAPITOLO 6
DATA RETENTION

CAPITOLO 7
LE ALTRE INDAGINI DIGITALI OCCULTE

CONSIDERAZIONI CONCLUSIVE

BIBLIOGRAFIA

«Le idee racchiuse in se stesse s'inaridiscono e si spengono. Solo se circolano e si mescolano, vivono, fanno vivere, si alimentano le une con le altre e contribuiscono alla vita comune, cioè alla cultura». G. Zagrebelsky, *Fondata sulla cultura: Arte, scienza e Costituzione*, 2014.

PREFAZIONE

Grazie all'informatica[1] negli ultimi venti anni la nostra società ha conosciuto una vera e propria rivoluzione tecnologica[2]: oggi, la maggior parte delle attività, sia di tipo lavorativo che sociale, di tipo pubblico o privato e personale, sfrutta una tecnologia di tipo digitale. La c.d. era digitale, che coinvolge oggi tutti gli aspetti della vita quotidiana, ha interessato anche il diritto, inteso come ordinamento del sociale.

In particolare sul piano del diritto penale sostanziale, l'avvento del digitale, oltre ad essere la causa di nuove figure delittuose[3], ha trasformato la fisionomia delle vecchie forme di criminalità, determinando una crescita esponenziale della frequenza con cui gli illeciti comuni sono perpetrati attraverso lo strumento informatico[4].

---

[1] Il termine "informatica", contrazione di informazione automatica, deriva dal termine tedesco *informatik* ed è stato coniato nel 1957 da K. STEINBUCH nel suo articolo *Informatik: automatische*. *Informationsverarbeitung*, poi ripreso da P. DREYFUS nel 1962 con il libro *Informatique*. L'etimologia italiana della parola "informatica" proviene dal francese, dalla compressione di *inform(ation électronique ou autom)atique*, e sicuramente P. DREYFUS, che per primo utilizza nel 1962 il termine *informatique* (informatica), voleva intendere il trattamento automatico dell'informazione mediante calcolatore (naturale o artificiale). Cfr. http://it.wikipedia.org/wiki/informatica. L'informatica, dunque, è la scienza che studia il trattamento delle informazioni mediante procedure automatizzabili ed eseguibili, quindi, tramite un elaboratore elettronico (in grado di elaborare informazioni espresse in forma numerica e che può pertanto definirsi "digitale"). Gli elementi fondamentali di un elaboratore digitale sono due, l'hardware ed il software: il primo indica la parte fisica di un computer ed è costituito da tutte quelle componenti elettroniche, elettriche, meccaniche, magnetiche, ottiche che ne consentono il funzionamento; il secondo, invece, è costituito da quei programmi, ossia algoritmi, che consentono al calcolatore di giungere da un input determinato ad un output determinabile. I programmi informatici sono costituiti, in estrema sintesi, da una sequenza di caratteri alfanumerici in grado di essere interpretati dal processore del computer come azioni da compiere al verificarsi di determinati presupposti di partenza. G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, Torino, 2012, p. 97.

[2] L'informatica, assieme all'elettronica e alle telecomunicazioni, unificate insieme sotto la denominazione *Information and Communication Technology (ICT)*, rappresenta quella disciplina e allo stesso tempo quel settore economico che ha dato vita e sviluppo alla terza rivoluzione industriale attraverso quella che è comunemente nota come rivoluzione informatica. Cfr. M. LUBERTO e G. ZANETTI. *Il diritto penale nell'era digitale. Caratteri, concetti e metafore,* in *Indice penale*, 2008, p. 497, dove gli ali autori paragonano l'avvento dell'era digitale alla prima rivoluzione industriale e alla bomba atomica.

[3] Si tratta dei c.d. *computer crimes* in senso stretto, previsti dalla legge 23 dicembre 1993, n. 547, recante modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, su cui poi è intervenuta la legge 18 marzo 2008, n. 48. In questa tipologia di reati, il sistema informatico rappresenta uno degli elementi costitutivi dell'illecito. Basti pensare, a titolo di esempio, al danneggiamento di informazioni, dati e programmi informatici (art. 615-*bis* c.p.), all'accesso abusivo ad un sistema informatico (art. 615-*ter* c.p.) o alla frode informatica (art. 640-*quinquies* c.p.).

[4] Si tratta dei c.d. *computer-related crimes.* Cfr. V. APRUZZESE, *Dal computer crime al computer-related crime,* in *Rivista di criminologia, vittimologia e sicurezza*, 2007, pp. 55 e ss. Si pensi, a titolo di esempio, alla diffamazione on line, alla estorsione telematica, alla pedopornografia in rete, ecc.: «*Internet* ed i nuovi prodotti tecnologici, infatti, possono certamente costituire sia il mezzo tipico per la commissione di taluni illeciti, sia l'oggetto passivo di questi ultimi. Ma oltre a queste ipotesi, sistematicamente inquadrabili nella categoria dei "reati informatici in senso proprio", sono molteplici i "comuni" fatti criminosi che possono essere commessi

Tuttavia, l'aspetto più problematico della c.d. "rivoluzione digitale" si coglie dal punto di vista processuale e consiste nel fatto che la prova -rappresentativa, sub specie documentale, di tipo reale- di qualsiasi tipo di illecito, finisce ormai quasi sempre per annidarsi in dispositivi di memorizzazione virtuale delle informazioni[5]. Il *computer*, inteso in senso lato, ha smesso di rilevare esclusivamente come elemento costitutivo della fattispecie (ossia oggetto su cui cade la condotta criminosa) o come mezzo attraverso il quale viene realizzato l'illecito[6], per acquisire sempre maggiore importanza quale fonte di prova[7] in relazione a qualsiasi tipo di inchiesta penale, dalle indagini sul terrorismo a quelle per reati associativi, sino ai casi di omicidio[8]. In tutti questi casi «l'elaboratore elettronico viene in considerazione semplicemente come contenitore di informazioni che si suppongono utili a fini probatori»[9].

Ciò si traduce in una indiscutibile maggiore difficoltà di contrasto da parte delle autorità investigative, direttamente proporzionale alle potenzialità (illimitate) offerte da Internet e dal mondo virtuale. Nel tentativo di rimanere al passo con i tempi, tale crescente difficoltà ha spinto ovviamente gli inquirenti verso nuove frontiere dell'investigazione, spesso toccando il limite che in uno Stato di diritto è rappresentato dal rispetto delle garanzie individuali[10].

---

mediante l'uso di strumenti informatici o telematici, non quali mezzi tipici di realizzazione dell'illecito, ma in quanto essi costituiscono una delle possibili modalità che in concreto sono utilizzate dagli autori dei crimini o dai loro complici (si pensi, a tiolo d'esempio, ad attività preparatorie di scambi di informazioni in rete volte a pianificare e realizzare attacchi terroristici)». Così, R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online* durchsuchung, in *Riv. trim. dir. pen. eco.*, 2009, 3, p. 695. Cfr. anche S. ATERNO, *Modifiche al titolo III del libro terzo del codice di procedura penale,* in AA.VV., *Cybercrime, responsabilità degli enti, prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, a cura di G. CORASANTI - G. CORRIAS LUCENTE, Padova, 2009, pp. 193 ss.; R. FLOR, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet*, su *www.penalecontemporaneo.it.*

[5] «Il diritto si sta muovendo sempre di più verso la digitalizzazione, nel senso che nella società odierna, anche nel corso delle indagini correlate a reati tradizionali, vengono in essere, quasi sempre, aspetti tecnologici. Non appare peregrina l'affermazione o, meglio, la previsione, che nel prossimo futuro qualsiasi tipo di fonte di prova sarà "digitale", in quanto il processo di informatizzazione e digitalizzazione della nostra società condizionerà direttamente il mondo giuridico e, soprattutto, il suo aspetto processuale». Così, G. ZICCARDI, *Le tecniche informatico giuridiche di investigazione digitale*, in *Investigazione penale e tecnologia informatica*, Milano, 2007, p. 9.

[6] In tali casi, evidentemente, «l'elaboratore elettronico può essere oggetto di sequestro *ex* art. 253, comma 2, c.p.p., senza particolari problemi, identificandosi nel corpo del reato». Così. F. M., *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2012, p. 697.

[7] Per una panorama completo sulle diverse coniugazioni del termine "prova", cfr. P. TONINI, *Manuale di procedura penale*, XVI ed., Milano, 2015, pp. 225 e ss.

[8] Basti pensare all'alibi informatico di Alberto Stasi nel caso del processo per l'omicidio di Garlasco per avere un'idea di come e quanto, ormai, l'informatica è entrata prepotentemente a far parte del lavoro di indagine e, più in generale, del bagaglio culturale di tutte le parti coinvolte nel processo.

[9] F. M. MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico,* cit., p. 697.

[10] Cfr. O. MAZZA, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, Relazione al convegno di studi su *Garanzia dei diritti fondamentali e processo penale*, organizzato da Diritto penale contemporaneo, Magistratura Democratica e la Camera Penale di Milano il 9 e 10 novembre 2012 presso l'Aula Magna del Palazzo di Giustizia di Milano, www.penalecontemporaneo.it, 30 novembre 2015.

In particolare, le indagini informatiche si caratterizzano e si distinguono da quelle tradizionali per almeno tre ragioni fondamentali: 1) la promiscuità dei dati; 2) l'impossibilità di un accesso selettivo al sistema informatico; 3) il loro oggetto, uno spazio (informatico) globale refrattario a qualsiasi tipo di limitazione nazionale.

Quanto alla prima caratteristica, i sistemi informatici sono sistemi complessi che contengono una pluralità di dati, consistenti sostanzialmente in informazioni, di diversa natura, in grado di circolare con estrema rapidità e facilità, prive di una dimensione fisica e duplicabili su più supporti. Seconda caratteristica: al contrario di ciò che avviene normalmente nel corso di indagini tradizionali, allo stato la tecnica non consente di limitare la ricerca a specifici dati o a specifiche informazioni.

Le conseguenze di queste prime due caratteristiche sono presto dette: le indagini informatiche sono sempre lesive della riservatezza delle persone coinvolte e della sicurezza dei dati contenuti nei sistemi informatici; inoltre, alto è il rischio che tali attività si trasformino in attività esplorative volte alla ricerca delle notizie di reato (c.d. indagini pro-attive: indagini ad alto contenuto tecnologico che si pongono a metà strada tra la prevenzione e la repressione).

La terza caratteristica fondamentale delle indagini informatiche attiene al loro oggetto: i dati digitali sono spesso salvati su *server* o su *personal computer* dislocati in paesi diversi rispetto a quello dove si svolgono le indagini, spesso si tratti di dati salvati nel *cloud*, e quindi si pongono dei seri problemi di cooperazione giudiziaria che richiedono sicuramente un aggiornamento degli strumenti di cooperazione ma anche, nei limiti in cui ciò è possibile, uno sforzo di armonizzazione delle definizioni normative degli strumenti investigativi, in modo da evitare una sorta di *far west* tecnologico in cui ogni Stato conduce indagini oltre la propria sovranità fino a dove la tecnologia lo consente.

Nel processo penale lo scontro tra nuove forme di criminalità e nuove metodologie investigative di contrasto si traduce nel continuo sforzo del legislatore[11] e dell'interprete di conciliare due fondamentali ma opposte esigenze: l'accertamento del fatto e la tutela dei diritti fondamentali degli individui coinvolti in tale accertamento. Il *punctum dolens* è sempre lo

[11] Con l'entrata in vigore del Trattato di Lisbona la "criminalità informatica" è stata inserita nell'art. 83 TFUE fra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione Europea ha competenza penale.

stesso: saper trovare un giusto equilibrio tra tutela della società e rispetto dei diritti fondamentali della persona[12].

Anche con riferimento al digitale, sorge la necessità di conciliare innovazioni scientifiche e rispetto delle regole processuali, fra le quali soprattutto la garanzia del contraddittorio nella formazione della prova[13], vero e proprio antidoto rispetto alle incertezze connaturate ad una scienza passibile di confutazione in qualsiasi momento[14]. L'informatica, infatti, non sfugge alla fallibilità che caratterizza tutte le branche del sapere e l'evidenza elettronica, lungi dall'essere "prova perfetta", racchiude e riacutizza le criticità già insite nella prova scientifica[15]. In tema di *digital evidence,* l'elevata connotazione specialistica della materia, insieme al concreto pericolo di manipolazione e di alterazione del materiale probatorio e al rischio di una incontrollata introduzione di una *junk science*, sono problematiche che richiedono estrema cautela: l'interprete è tenuto a verificare con rigore la compatibilità degli strumenti offerti dal progresso scientifico rispetto ai principi cardini del processo penale, primo fra tutti la garanzia del diritto di difesa, inviolabile in ogni stato e grado del procedimento[16].

A livello epistemologico, infatti, è necessario ancora una volta sfatare il mito della prova scientifica come "prova perfetta"[17]: nel processo penale, il sapere specialistico non deve ergersi a roccia contro la quale sono destinate ad infrangersi le più elementari garanzie partecipative dei soggetti coinvolti nell'accertamento penale, ma deve essere come acqua

---

[12] Cfr. S. LORUSSO, *L'arte di ascoltare e l'investigazione penale tra esigenze di giustizia e tutela della privatezza*, in *Dir. pen. proc*., 2011, 11, pp. 1397 ss. Più in generale, C. CONTI - P. TONINI, *Il diritto delle prove penali*, Milano, 2012, p. 5.

[13] Nella consapevolezza che «Noi corriamo verso un ideale di Giustizia, anche se esso è paradossalmente irraggiungibile come la tartaruga per Achille. Non dobbiamo mai smettere di correre, nel rispetto delle regole e delle garanzie. La Giustizia s'incontra nel percorso, prima ancora che alla meta». C. CONTI - P. TONINI, *Il diritto delle prove penali*, cit., in epigrafe.

[14] Come noto, la crisi dell'equazione tra scienza e episteme si deve al pensiero di K.R. POPPER, che segna definitivamente il declino del verificazionismo come metodo gnoseologico. Alla filosofia popperiana si deve la ormai acquisita consapevolezza di una scienza come sapere non più indebitamente certo, ma limitato, incompleto e fallibile. CFR. K.R. POPPER, *Logica della scoperta scientifica*, Torino, 1970.

[15] «Si comprende bene allora che i problemi che sorgono quando si parla di investigazioni informatiche non siano solamente di carattere strettamente tecnico, ma anche e soprattutto epistemologico: non basta infatti limitarsi a individuare le soluzioni tecniche più idonee a estrapolare da un elaboratore elettronico il maggior numero di informazioni, occorrendo invece che tali attività siano correttamente inquadrate all'interno del sistema probatorio, e svolte conformemente alle regole che lo disciplinano, così da garantire una ricostruzione del fatto il più possibile approssimata alla realtà e la tutela dei diritti individuali coinvolti». Così, F. M. MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, cit., p. 698.

[16] E. LORENZETTO, *Le attività urgenti di investigazione informatica*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, p. 137.

[17] Per tutti, cfr. O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005.

capace di modellarsi e adeguarsi al contenitore in cui viene versata, un contenitore la cui natura giuridica e processuale richiede il rispetto di regole a tutela dei diritti involabili della persona. D'altronde, è la stessa espressione "prova scientifica" a imporre questo ordine di idee: la parola "scientifica" rimanda al concetto di scienza, ma viene dopo il termine "prova", il quale rinvia a norme e principi contenuti sia nel codice di rito che in Costituzione, cogenti *erga omnes* con forza vincolante.

Nella fase delle indagini preliminari la prima e fondamentale garanzia della difesa, espressione di quel concetto di contraddittorio oggettivo, seppur debole, menzionato dall'art. 111, comma 2, Cost., è rappresentata dalla "conoscibilità"[18] dell'atto investigativo. Ebbene, proprio facendo perno sul requisito della conoscibilità, le indagini tecnologiche di natura digitale possono essere distinte in due grandi categorie: indagini palesi e indagini occulte (o segrete).

Alla partizione delle indagini palesi appartengono strumenti di ricerca della prova essenzialmente tipici: rilievi e accertamenti urgenti, ispezioni, perquisizioni e sequestri, così come novellati dalla legge 18 marzo 2008, n. 48[19]. Con riferimento a tale tipologia di attività, possiamo parlare di "aspetto statico" della prova informatica.

Quanto alle indagini occulte, le quali rappresentano l' "aspetto dinamico" della prova digitale[20], è necessario distinguere ulteriormente tra indagini tipiche e indagini atipiche: nell'ambito del primo gruppo è possibile ricomprendere le intercettazioni telematiche, le

---

[18] Lo svolgersi del processo penale genera un contrasto tra opposte esigenze. Vi è la necessità di proteggere la ricerca della verità contro gli atti che possono mettere in pericolo l'acquisizione o la genuinità della prova; ma vi è anche quella di assicurare l'esercizio del diritto di difesa. Per gli atti di indagine compiuti dal pubblico ministero e dalla polizia giudiziaria è previsto come regola l'obbligo del segreto (art. 329, comma 1, c.p.p.). Alla regola della segretezza, tuttavia, sono state poste varie deroghe in favore della difesa: gli atti garantiti e gli atti a sorpresa, infatti, sono "conoscibili" dall'indagato. Cfr. P. TONINI, *Manuale di procedura penale*, cit., pp. 500 e ss.

[19] L. 18-3-2008 n. 48 - Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno. Pubblicata nella Gazz. Uff. 4 aprile 2008, n. 80, S.O. Prima di tale novella normativa, l'ispezione, la perquisizione ed il sequestro di evidenze digitali erano considerati mezzi "atipici" di ricerca della prova. Con la legge n. 48 «tutto è ricondotto alla tipicità con opportuni adeguamenti». Così, P. TONINI, *Manuale di procedura penale*, cit., p. 378. Per un primo esaustivo commento alle modifiche processuali introdotte dalla legge 18 marzo 2008, n. 48 - *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno* -, cfr. S. ATERNO, *Modifiche al titolo III del libro terzo del codice di procedura penale,* cit., pp. 193 e ss.; P. TONINI, *Documento informatico e giusto processo,* in *Dir. pen. proc.*, 2009, p. 401. Quanto agli aspetti sostanziali della novella, cfr. P. SCOGNAMIGLIO, *Criminalità informatica. Commento organico alla Legge 18 marzo 2008, n. 48*, Napoli, 2008.

[20] Il dato digitale può essere colto sia nella sua dimensione dinamica, cioè mentre fluisce, ma anche quando è conservato in *server* pubblici, privati, o semplicemente su dispositivi che appartengono alla vita quotidiana di tutti noi. Sulla distinzione tra prova digitale *off line* e prova digitale *on line*, sia consentito rinviare a C. CONTI - M. TORRE, *Spionaggio informatico nell'ambito dei social network*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, pp. 402 e ss.

intercettazioni ambientali tramite *virus* informatico, le operazioni digitali sotto copertura[21] ed il monitoraggio dei siti Internet, anche alla luce delle novità introdotte dalla recente normativa antiterrorismo[22]; nell'ambito delle indagini digitali atipiche, invece, viene in rilievo il fenomeno del cd. "captatore informatico"[23], sempre più spesso utilizzato dagli inquirenti in ragione della enorme quantità e qualità di informazioni estrapolabili, oltre al c.d. "pedinamento elettronico" ed alle videoriprese tramite *virus* informatico.

Sulla prova informatica nel processo penale le questioni ad oggi aperte sono molteplici e tutte caratterizzate da notevole complessità. In questo contributo, partendo dalla definizione stessa dell'istituto -sulla quale, come vedremo, manca unanimità di vedute fra gli interpreti- si passeranno in rassegna le principali problematiche connesse, rispettivamente, al profilo statico ed al profilo dinamico dell'acquisizione dell'evidenza digitale a scopo investigativo e probatorio.

In particolare, nella prima parte dell'elaborato si affronta il tema della acquisizione della prova digitale *off line.* Come noto, si tratta della fase maggiormente problematica nella gestione della *digital evidence*. Qui, il terreno di scontro fra dottrina e giurisprudenza è squisitamente tecnico ed è rappresentato dalla divergenza di opinioni circa la natura ripetibile o non ripetibile dell'attività di acquisizione dei file on site, in sede di sopralluogo (art. 354, co. 2, c.p.p.), ispezione (art. 244, co. 2, c.p.p.), perquisizione (artt. 247, co. 1-*bis* e 352, co. 1-

---

[21] Disciplinate dall'art. 9 della legge 16 marzo 2006, n.146 (Legge di ratifica della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale) e dall'art. 14 della legge 3 agosto 1998, n. 269 (Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù), così come integrato dalla legge 6 febbraio 2006, n. 38 (Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo *Internet*), il cui art. 16, comma 3, prevede che: «Le disposizioni di cui all'articolo 14 della legge 3 agosto 1998, n. 269, si applicano anche quando i delitti di cui all'articolo 600-*ter*, commi primo, secondo e terzo, del codice penale sono commessi in relazione al materiale pornografico di cui all'articolo 600-*quater* del medesimo codice». Cfr. F. CAJANI, *Le operazioni digitali sotto copertura: l'agente provocatore e l'attività di contrasto nelle indagini informatiche*, in S.ATERNO-F.CAJANI-G. COSTABILE-M. MATTIUCCI-G. MAZZARACO (a cura di), *Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Forlì, 2011, pp. 411 ss.

[22] D.L. 18 febbraio 2015, n. 7, così modificato dalla legge di conversione 17 aprile 2015, n. 43.

[23] Come si vedrà *amplius infra*, si tratta di *software* in grado di captare i dati e di trasmetterli, in tempo reale o ad intervalli prestabiliti, agli organi di investigazione. Su questo particolare e nuovo strumento di indagine, vedi S. MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in *Cass. pen.*, 07/08, 2010, pp. 2855 e ss. Cfr., inoltre, S. ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del cloud criminal*, in G. COSTABILE - A. ATTANASIO (a cura di), *IISFA Memberbook 2012 Digital Forensics. Condivisione della conoscenza tra i membri dell'IISFA Italian Chapter*, Forlì, 2013, pp. 1 e ss. Per una analisi comparata: con specifico riferimento all'esperienza tedesca, cfr. R. FLOR, *La sentenza del Bundesverfassungsgericht del 27 febbraio 2008 sulla c.d. online* durchsuchung, cit., pp. 679 e ss.; quanto all'esperienza statunitense, v. F. CERQUA, *Le investigazioni informatiche e la protezione dei dati personali negli Stati Uniti ed in Italia: due modelli a confronto*, in P. CORSO - E. ZANETTI, (a cura di), *Studi in onore di Mario Pisani, II, Diritto processuale penale e profili internazionali: diritto straniero e diritto comparato*, Piacenza, 2010, pp. 775 e ss.

bis c.p.p.) e sequestro (art. 254-*bis* c.p.p.) Nell'ambito delle operazioni tecniche non ripetibili, inoltre, è necessario distinguere tra accertamenti modificativi della fonte di prova e accertamenti modificativi degli elementi di prova, essendo diverse le rispettive norme di copertura. Punto di partenza della nostra riflessione è la legge 18 marzo 2008, n. 48: è facile osservare che il codice di procedura penale, all'indomani della novella, si occupa di prova digitale attraverso la rivisitazione di istituti tipici vecchi. La tecnica legislativa utilizzata per fare spazio alla *digital evidence* all'interno del codice di rito è stata quella di integrare le vecchie disposizioni previste per le ispezioni, le perquisizioni e i sequestri attraverso la previsione di una formula tautologica comune a tutti e tre i mezzi di ricerca della prova citati: «adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»[24]. Come vedremo, il problema è che in ambito informatico è naturalisticamente difficile distinguere tra accertamento, ispezione, perquisizione e sequestro[25]. Probabilmente sarebbe stato più opportuno predisporre un nuovo strumento di ricerca *ad hoc* per la prova di natura digitale, disciplinando in modo più dettagliato le attività da compiere per assicurarne il valore probatorio. Probabilmente, la fretta dovuta alla necessità di far fronte alle scadenze europee è stata cattiva consigliera e così la novella normativa del 2008 si è tradotta in un "copia e incolla" normativo (dalla fonte europea alla legge italiana) che non ha tenuto conto delle specificità della realtà scientifica di riferimento. In altre e più semplici parole, si sono voluti regolamentare istituti nuovi ragionando con schemi vecchi, senza tener conto del fatto che in ambito informatico non è possibile riuscire a distinguere tra ispezioni, perquisizioni e sequestri: l'unica cosa che conta è l' "apprensione" dell'evidenza digitale con metodi e tecniche idonei a conciliare accertamento del fatto e garanzie individuali. Utilizzando le vecchie norme sugli accertamenti urgenti, sulle ispezioni, le perquisizioni ed il sequestro il legislatore della novella ha creato delle problematiche interpretative di non poco conto, destinate ad emergere ogni qual volta si cerchi di inquadrare una determinata attività operativa nell'una o nelle altre fattispecie previste dal codice, con evidenti conseguenze in termini di disciplina applicabile e di pretese garanzie[26].

---

[24] Cfr. artt. 244, comma 2; 247, comma 1-*bis;* 352, comma 1-*bis*; 354, comma 2, c.p.p.

[25] Si potrebbero, al più, proporre i seguenti criteri: 1) se l'accesso ai dati digitali è libero, allora si tratta di ispezione; se è necessaria una password, allora si tratta di perquisizione; 2) ispezione vuol dire guardare l'hardware; perquisire significa entrare e guardare i dati; 3) ispezione significa guardare i metadati; perquisire invece guardare i dati ed il loro contenuto.

[26] In senso critico sulla tecnica dell'interpolazione e sulla sottesa scelta di adattare i tradizionali mezzi di ricerca della prova alla raccolta del dato digitale, anziché introdurne di specifici, v. L. LUPARIA, *La ratifica della*

La seconda parte del presente lavoro è dedicata all'approfondimento –anche in una prospettiva *de iure condendo*- del tema delle investigazioni informatiche *online*. Tale argomento coinvolge la questione della legittimità delle indagini atipiche e della conseguente utilizzabilità dei suoi risultati, con specifico riferimento ai limiti derivanti dalle regole di esclusione di matrice costituzionale. Come vedremo, salvo ipotesi particolari[27] nella prassi giudiziaria è difficile che emerga un problema che coinvolga esclusivamente la prova atipica; il vero dilemma sono le indagini atipiche, ossia quelle attività investigative completamente sciolte da briglie di natura positiva. Da questa prospettiva, la novella normativa del 2008 è stata un'occasione mancata, non avendo il legislatore distinto tra prova informatica *off line* e prova informatica *online* (la prima conservata sulla memoria di massa del computer o su strumenti di tipo integrativo di questa, quali CD, DVD, USB, ecc.; la seconda accessibile mediante rete telematica). In particolare, quest'ultimo aspetto relativo al profilo dinamico della prova digitale non è stato affatto disciplinato; sarebbe stato invece opportuno prevedere anche tale tipo di captazione digitale attraverso uno strumento tipico *ad hoc*, in maniera non troppo diversa da quanto oggi avviene con riferimento alle intercettazioni delle conversazioni telefoniche ed ambientali, con dettagliate discipline dei casi e dei modi in cui è ammessa l'intrusione investigativa[28].

Per questo motivo, al termine di un appassionato capitolo interamente dedicato al c.d. "captatore informatico", l'autore allega una propria proposta di inserimento, nel Libro III, Titolo III, del codice di procedura penale, di un capo V (artt. 271-*bis* – 271-*sexies*) dedicato ai "Programmi informatici per l'acquisizione da remoto dei dati e delle informazioni presenti in un sistema informatico o telematico", modellandone chiaramente la disciplina sulla base di quanto previsto in materia di intercettazioni, seppur con qualche spunto di novità. Nei successivi capitoli si passano in rassegna le altre tipologie di indagini digitali occulte, attualmente in voga nella prassi operativa, non senza sottolinearne relative criticità: intercettazioni telematiche; pedinamento elettronico; data retention; indagini *under cover* e monitoraggio dei siti; cloud computing; Osint.

Questa poco rassicurante premessa non scoraggi il lettore. Nel prosieguo di questo lavoro ci si soffermerà su ciò che il Legislatore ha scritto e su ciò che non ha scritto (o voluto

---

Convenzione cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. I profili processuali, in *Dir. pen. proc*., 2008, p. 718.

[27] Per esempio, la perizia fondata su una nuova scienza o il problema della neuro-scienza.

[28] Auspicava ed auspica tale soluzione, fra gli altri, S. MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, cit., pp. 2855 e ss.

scrivere). Dopo l'esame e la critica, tuttavia, saranno proposte delle soluzioni concrete, opinabili certamente, ma presenti e praticabili. L'idea che ha sostenuto lo scrivente è semplice: il divieto di *non liquet* dovrebbe valere non soltanto per il giudice, ma anche e soprattutto per chi, ad ogni livello, quel giudice o quel legislatore intenda (giustamente) criticare. Solo così la critica diviene costruttiva e foriera di una scienza giuridica degna di tale nome.

PARTE PRIMA
INDAGINI INFORMATICHE CONOSCIBILI:
LA PROVA DIGITALE *OFF LINE*

CAPITOLO 1
PROVA INFORMATICA E PROCESSO PENALE

Sommario: 1. *Scripta manent, data quoque* – 2. Documento e documentazione - 3. Sulla definizione giuridica di documento, dall'analogico al digitale – 4. Prova scientifica e processo penale

1. *Scripta manent, data quoque*

Il processo penale tenta, pur con inevitabile approssimazione, di raggiungere la verità circa l'*an* e il *quomodo* di fatti avvenuti in passato e giuridicamente rilevanti per la legge penale. Tuttavia, il risultato conoscitivo ottenuto all'esito del rito penale, noto come "verità processuale", per motivi fisiologici e non patologici non corrisponderà mai alla "verità storica". Tale corrispondenza rappresenterebbe un'utopia, poiché la verità storica coincide con avvenimenti avvenuti in passato e che sono impossibili da recuperare nel presente[29]; d'altronde, ogni fatto umano è irripetibile per il fatto stesso di essere accaduto, trattandosi di un *unicum* storico che appartiene alla storia (*lost fact*). La verità processuale tenta di ricostruire, mediante le prove, i fatti accaduti nel passato[30]; il processo, quindi, non si pone come obiettivo quello di recuperare, con tutti i mezzi a disposizione, un fatto appartenente al passato, ma ha un fine più concreto, che consiste nella ricostruzione (rappresentativa o indiziaria) di quel fatto attraverso strumenti controllabili -le prove- al precipuo scopo di affermare o negare una determinata responsabilità penale. Ergo, la vera differenza tra le due verità è rappresentata dalla intermediazione delle prove e delle regole di esclusione che le governano: la verità storica ne fa volentieri a meno; la verità processuale erge il diritto delle prove a fulcro del processo penale.

Ebbene, un sistema processuale basato sul modello inquisitorio giudica la dettagliata disciplina del diritto delle prove un ostacolo verso quel percorso di avvicinamento della verità processuale alla verità storica. Nel sistema accusatorio, invece, è matura la consapevolezza che la legalità processuale e, in particolare, il diritto delle prove ed il principio del

[29] Non esistono limiti alla ricerca della verità storica: il fine giustifica i mezzi ed ogni mezzo idoneo alla ricostruzione di tale verità è, per ciò solo, ammissibile e utilizzabile.
[30] Tale ricostruzione è limitata dalle regole probatorie e di giudizio che operano nel processo penale: il fine è condizionato dai mezzi e dalle regole di esclusione proprie del rito.

contraddittorio rappresentano non soltanto una garanzia per i soggetti coinvolti nell'accertamento processuale, ma anche e soprattutto il miglior metodo oggettivo per ricostruire oggi fatti che ormai appartenengono al passato. Tale differenza, probabilmente, è all'origine della divaricazione concettuale tra i due sistemi processuali.

D'altronde, la verità processuale è ciò che esce dal processo, non ciò che preesiste ad esso (verità storica). Ecco cos'è il processo: è il percorso per accertarla, il *rewind*, perché dal presente risale al passato. Ma -ed è questa la linea di confine tra un sistema inquisitorio ed uno accusatorio- il processo non può e non deve avere una "conoscenza onnivora", quanto piuttosto una "conoscenza selettiva", che consenta di giungere ad una decisione definitiva -giusta o sbagliata che sia- veicolata attraverso opportuni sistemi di controllo. Il primo e fondamentale strumento di selezione e controllo è rappresentato dal principio del contraddittorio nella formazione della prova, dichiarativa o reale che sia[31].

Come noto, l'opera di ricostruzione di un fatto può giovarsi di rappresentazioni e indizi. L'inferenza rappresentativa, a sua volta, può essere di tipo dichiarativo (testimonianza) o reale (documento) [32]. In quest'ultima dicotomia è possibile cogliere quel paradosso[33] che da sempre caratterizza la cultura occidentale[34] e che riverbera inevitabilmente i suoi effetti anche nel processo penale, persino di tipo accusatorio: da un lato, si enfatizza il ruolo e la portata del principio di oralità, la cui massima espressione, in tema di formazione della prova, si raggiunge nell'esame del testimone in contraddittorio fra le parti attraverso l'esame incrociato[35]; dall'altro lato, subdola ma incalzante, resiste l'idea che le «registrazioni …

---

[31] Ed infatti, l'art. 111 Cost., al 2° comma, stabilisce che «Nel processo penale la legge assicura che la persona accusata di un reato sia, nel più breve tempo possibile, informata riservatamente della natura e dei motivi dell'accusa elevata a suo carico; disponga del tempo e delle condizioni necessari per preparare la sua difesa; abbia la facoltà, davanti al giudice, di interrogare o di far interrogare e persone che rendono dichiarazioni a suo carico, di ottenere la convocazione e l'interrogatorio di persone a sua difesa nelle stesse condizioni dell'accusa [contraddittorio sulla prova dichiarativa, n.d.r.] e l'acquisizione di ogni altro mezzo di prova a suo favore [contraddittorio sulla prova reale, n.d.r.]».

[32] Per un approfondimento sulla distinzione tra prova rappresentativa e prova indiziaria o critica, si rinvia a P. TONINI, *Manuale di procedura penale,* cit., pp. 225 e ss.

[33] Parla, letteralmente, di "paradosso" F. ZACCHÈ, *La prova documentale*, in G. UBERTIS - G.P. VOENA (diretto da), *Trattato di procedura penale*, XIX, Milano, 2012, p. 5.

[34] Cfr. U. VOLLI, *Il nuovo libro della comunicazione. Che cosa significa comunicare: idee, tecnologie, strumenti, modelli*, Milano, 2007, p. 131, nel quale si può leggere come, per Platone, l'«oralità implic[hi] la presenza degli interlocutori, quindi dialogo, possibilità per chi parla di "difendere il discorso". La scrittura al contrario implica assenza, quindi impossibilità del dialogo: il libro, interrogato, non risponde o ripete sempre la stessa cosa»

[35] «Questo istituto può essere definito come quell'insieme di regole con le quali le parti pongono direttamente le domande alla persona esaminata». Cfr. P. TONINI, *Manuale di procedura penale*, cit., p. 698.

forniscano prove più sicure della parole parlate, specie in tribunale»[36], giacché «il sapere scritto è anche il sapere per eccellenza»[37].

La genesi del paradosso è dovuta, a parere di chiscrive, al difficile equilibrio tra due opposti interessi, entrambi meritevoli di tutela: da un lato, il principio dialettico nella formazione della prova, inteso come lo strumento migliore, o il meno imperfetto, per stabilire la verità di determinati enunciati fattuali; dall'altro, il principio di non dispersione della prova, grimaldello idoneo a consentire importanti eccezioni al contraddittorio orale fra le parti. Proprio in virtù del fatto che non si è disposti a smarrire alcun tipo di informazione utile ai fini delle indagini, «ogni nozione che non sia di uso immediato […] si tramuta in documento di una qualche forma»[38]

Ed allora, il modo migliore per sciogliere il paradosso consiste nell'attribuire al documento il ruolo che gli compete all'interno del sistema, sì da valorizzarne gli aspetti positivi senza tuttavia lasciarsi condizionare da quelli negativi, individuando regole di utilizzabilità e regole di esclusione: nel fare ciò, come Ulisse, è necessario rimanere legati all'albero maestro della nave, in modo tale da sentire il canto meraviglioso ma ingannevole delle sirene senza esserne tuttavia fatalmente attratti sino al punto di finire sugli scogli. Infatti, nemmeno il documento sfugge alle insidie della fallibilità umana ed il progresso tecnologico, in questo campo, riacutizza le problematiche che da tempo ormai caratterizzano il tormentato rapporto tra scienza e processo[39].

D'altronde, del documento e del documento informatico in particolare, non è più possibile fare a meno. Ciò non solo e non tanto perché negli ultimi anni è definitivamente caduto il dogma della prevalente importanza della prova dichiarativa rispetto alla prova reale[40], ma anche e soprattutto in ragione del fatto che la nostra è una società mediata dalla scrittura e, attualmente, dalla diffusione capillare di dati digitali, atteso che nel mondo in cui viviamo la maggior parte degli eventi lascia traccia in un documento, analogico o informatico. E' questo

---

[36] W. J ONG, *Oralità e scrittura. Le tecnologie della parola*, Bologna, 1986, p. 139.
[37] G.R. CARDONA, *Antropologia della scrittura*, Torino, 2009, p. 102.
[38] *Ibidem.*
[39] Cfr. O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, cit., p. 11; S. LORUSSO, *La prova scientifica*, in *La prova penale*, trattato diretto da A. GAITO, Torino, 2008, p. 796; P. TONINI, *Dalla perizia "prova neutra" al contraddittorio sulla scienza,* in *Dir. pen. proc.*, 2011, p. 11.
[40] Anzi, è vero il contrario: lo studio della psicologia della testimonianza ci insegna che la prova dichiarativa è per definizione una prova debole, perché, a prescindere dal caso della dichiarazione dolosamente falsa, essa è soggetta a gravi fattori di distorsione che possono influire sulla stessa. Viceversa, la prova rappresentativa di tipo reale costituisce, oggi, il perno di ogni indagine e, spesso, segna il discrimine tra un esito assolutorio o di condanna.

il motivo per cui il legislatore del codice del 1988 ha dedicato alla prova documentale un intero capo (VII) del Titolo II del Libro III del codice di procedura penale, con l'obiettivo di dare omogeneità a una disciplina che, nel codice di procedura penale del 1930, era frammentaria e disorganica. Ed è su questa disciplina che, da ultimo, nel 2008, è intervenuto nuovamente il legislatore modificando il codice per fare spazio, al suo interno, alla nuova realtà rappresentata dal "documento informatico" o, volendo usare una terminologia di matrice anglosassone, dalla *digital evidence*[41].

---

[41] Non esiste una definizione univoca di *digital evidence*, né a livello internazionale, né a livello di diritto domestico.
A livello internazionale, tra le varie definizioni adottate meritano di essere ricordate quella della *International Organization on Computer Evidence* (la IOCE è un'organizzazione internazionale costituita nel 1998 con l'obiettivo di creare un luogo di dibattito, di confronto e di scambio di informazioni tra le forze dell'ordine di tutti gli Stati aderenti), secondo la quale la *electronic evidence* «è un'informazione generata, memorizzata e trasmessa attraverso un supporto informatico che può avere valore in tribunale» (definizione adottata dalla IOCE nel 2000 e poi ripresa dal Consiglio d'Europa nel 2013), nonché quella adottata dallo *Scientific Working Group on Digital Evidence* (la SWGDE è un'organizzazione internazionale costituita nel 1998 che raccoglie tutte le organizzazioni attivamente coinvolte nel settore della prova digitale e nel settore multimediale al fine di promuovere la cooperazione e di garantire la qualità nel settore della ricerca della prova digitale) , secondo cui *digital evidence* è «qualsiasi informazione, con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale» (Definizione adottata nel 1999 da SWGDE all'interno del *Document Digital Evidence*: *Standards and Principles*, disponibile al seguente URL: http://www.fbi.gov/about-us/lab/forensics-scienze-communications/fsc/april2000/swgde.htm). In realtà, la *electronic evidence* rappresenta un *genus* più ampio in cui è possibile sussumere le diverse *species* della *analogue evidence* e della *digital evidence*. In particolare, "prova elettronica" è «l'insieme di tutti quei dati, inclusi quelli derivanti dalle risultanze registrate da apparati analogici e/o digitali, creati, processati, memorizzati o trasmessi da qualsiasi apparecchio, elaboratore elettronico o sistema elettronico, o comunque disseminati a mezzo di una rete di comunicazione, rilevanti ai fini di un processo decisionale» (S. Mason, *Electronic Evidence. Discovery & Admissibility*, LexisNexis Butterwoorths, Londra, 2007, par. 2.03). "Prova digitale", invece, è il solo dato informatico, dal quale si «possa stabilire se un crimine è stato commesso o che può fornire un collegamento tra il crimine e chi l'ha commesso» (E. CASEY, *Digital Evidence and Computer Crime*, II ed., Elsevier, 2004, p. 12). Anche il Consiglio d'Europa, nel 2013, si occupa di *digital evidence* e lo fa, innanzitutto, a scopo definitorio: «le fonti di prova digitale sono informazioni generate, memorizzate o trasmesse mediante dispositivi elettronici che possono essere utilizzate in giudizio» (Consiglio d'Europa, Guida alla prova digitale. Linee guida per polizia giudiziaria e autorità giudiziaria, Strasbourg, 18 marzo 2013, www.coe.int/cybercrime).
A livello di diritto interno, il legislatore, nel tentativo di definire il mezzo di prova "documento informatico", ha cambiato idea per ben tre volte negli ultimi quindici anni dimostrando di non aver le idee troppo chiare sull'argomento. Nel 1993, la prima definizione di documento informatico, utile anche a fini processuali, si deve ad una esigenza tipica di diritto penale sostanziale: estendere l'incriminazione del falso documentale al dato informatico, onde evitare pericolosi vuoti di tutela. All'epoca, «[...] per documento informatico si intende[va] qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati ad elaborarli» (cfr. art. 491-*bis* c.p., inserito dalla l. 23 dicembre 1993, n. 547). Il problema è che si è cercato di utilizzare la tradizionale definizione civilistica di documento (Secondo la quale, appunto, con tale concetto si indicava un supporto), trapiantandola senza accorgimenti nel codice penale. La conseguenza, paradossale, è che dal punto di vista penalistico una simile definizione di documento informatico consentiva di tutelare il solo supporto fisico e non anche il dato informatico, vero oggetto degno di tutela («il documento informatico contiene dati immateriali, caratterizzati dalla fragilità. Se così è, la tutela penalistica sarebbe dovuta andare oltre il supporto fisico e avrebbe dovuto proteggere il dato informatico in se stesso contro le falsificazioni», P. TONINI, *Documento informatico e giusto processo*, cit., p. 402). In buona sostanza, definire il documento informatico come supporto fisico significa trascurare l'elemento della rappresentazione, vero fulcro del mezzo di prova in argomento. In base a questa interpretazione, la rappresentazione di un fatto non sta nel documento, ma in colui che, leggendo il documento, formula la decisione sull'esistenza del fatto (N. IRTI, *Sul*

Punto di partenza della riflessione, tuttavia, resta l'art. 111 Cost., il quale fa «assurgere il contraddittorio nella formazione della prova al rango di 'statuto epistemologico' della giurisdizione penale»[42]. Ebbene, rispetto al documento, ed in particolare rispetto al documento digitale, la coniugazione minima di tale principio diventa «riconoscere all'imputato il diritto di essere messo a confronto con il dato informatico nel suo aspetto genuino, senza alterazioni. Questa è la trasposizione moderna del diritto a confrontarsi con l'accusatore»[43]

E' indispensabile, inoltre, chiarire cosa si intenda per documento, fornendone una nozione e specificandone le diverse tipologie e classificazioni. Ed è questo che si tenterà di fare nei prossimi paragrafi, senza perdere di vista la meta, ossia la definizione di documento informatico.

2. Documento e documentazione

Non appare superfluo, in apertura di questo lavoro, sottolineare l'enorme differenza che esiste tra il concetto di "documento" e quello di "documentazione", e ciò non tanto e comunque non solo per puro esercizio accademico, che pure non dispiace in questa sede, ma

---

concetto giuridico di documento, in *Norme e fatti*, Milano, 1984, p. 249). L'inidoneità di tale definizione è stata percepita dalla unanime giurisprudenza che, di fatto, l'ha ignorata completamente (assimilando direttamente il documento informatico a quello tradizionale, di cui sarebbe al più una species, anziché un quid novum, in rapporto di analogia) sino a quando è stata definitivamente abbandonata nel 2008, con la legge n. 48 (Art. 3 l. 18 marzo 2008, n. 48: «All'articolo 491-*bis* del codice penale sono apportate le seguenti modificazioni: a) al primo periodo, dopo la parola: "privato" sono inserite le seguenti: "avente efficacia probatoria"; b) il secondo periodo è soppresso») . Nel frattempo, nel 2005, attraverso il Codice dell'amministrazione digitale (D. Lgs. 7 marzo 2005, n. 82), il legislatore aveva aggiornato la criticata definizione, chiarendo che per documento informatico si doveva intendere la rappresentazione informatica di un fatto giuridicamente rilevante. Il fine era buono, ma non è riuscito comunque a giustificare i mezzi: la parificazione del digitale all'analogico è avvenuta, infatti, attraverso la categoria concettuale dei "mezzi di rappresentazione". La nostra idea, invece, è che l'informatica, così come la scrittura, non sono modalità rappresentative di un fatto, quanto, piuttosto, "metodi di incorporamento". Il *gap* è notevole e divide la dottrina processual penalistica (Cfr. P. TONINI, *La prova penale*, 4ª ed., Padova, 2000, p. 193, nonché, ID., *Documento informatico e giusto processo*, cit., p. 402; G. UBERTIS, *Variazioni sul tema dei documenti*, in *Cass. pen.*, 1992, p. 2516. Di diverso avviso, P. CALAMANDREI, *La prova documentale*, Padova, 1997, p. 10, secondo il quale «documento ai fini del processo penale deve essere considerata ogni rappresentazione, anche non intenzionale, di un contenuto probatorio incorporato, anche non durevolmente, in una base»).

[42] O. MAZZA, *Le deroghe costituzionali al contraddittorio per la prova*, G. CONSO (a cura di), in *Il diritto processuale penale nella giurisprudenza costituzionale*, Napoli, 2006, p. 637; G. GIOSTRA, *Contraddittorio (principio del): II) diritto processuale penale*, in *Enc. giur. Treccani*, vol. IX, Roma, agg. 2001, p. 6.

[43] Così, P. TONINI, *Documento informatico e giusto processo*, cit., p. 406.

anche e soprattutto per ribadire regole probatorie di ammissibilità differenti, a seconda che si disquisisca dell'uno o dell'altra.

Già l'abrogato codice del 1930, seppur senza il dovuto rigore[44], differenziava a livello terminologico queste due tipologie documentali, riferendosi alla "documentazione" come "atti" e riservando il termine "documento" ai soli documenti extraprocessuali. Eppure, in un sistema processuale come quello del codice del 1930, dove la documentazione degli atti compiuti nelle fasi antecedenti al giudizio era pacificamente ammessa attraverso le letture dibattimentali, non c'era ragione alcuna per separare nettamente le due categorie concettuali.

Tale necessità, viceversa, si è imposta nella redazione del codice di procedura penale del 1988, che reagiva al precedente assetto normativo creando un sistema processuale prevalentemente accusatorio[45], basato, almeno sulla carta, sul principio della separazione delle fasi, giacché «in una prospettiva di riforma […] era indispensabile mettere ordine nella materia [quella documentale] e cercare di fissare strumenti concettuali precisi, in grado di orientare l'interprete»[46].

Dal punto di vista linguistico, il legislatore del 1988 ha fatto la medesima scelta del precedente codificatore, dedicando il termine "documenti" a quelli extraprocessuali ed impiegando il termine "atti" per i documenti processuali (la "documentazione")[47]. Dal punto di vista sistematico, le regole di ammissione nel processo dei documenti formati fuori dal procedimento trovano collocazione negli artt. 234-243 c.p.p., mentre la documentazione dell'attività processuale è disciplinata attraverso la normativa generale contenuta negli artt. 134-142 c.p.p. e la normativa speciale relativa al singolo tipo di atto; alla documentazione sono applicabili, inoltre, le norme del codice relative alla formazione dei fascicoli, alle letture

---

[44] Ad esempio, l'art. 463 c.p.p. del 1930, pur rubricato "atti e documenti", si riferiva in realtà ai soli documenti processuali; l'art. 466 del medesimo codice, invece, si riferiva indistintamente agli uni e agli altri. Cfr. *Relazioni al progetto preliminare e al testo definitivo del codice di procedura penale, delle disposizioni sul processo penale a carico di imputati minorenni e delle norme per l'adeguamento dell'ordinamento giudiziario al nuovo processo penale ed a quello a carico degli imputati minorenni*, in G.U. Serie Generale n. 250 del 24 ottobre 1988 - Suppl. Ordinario n. 93. Pacificamente in dottrina, cfr. S. CAMPANELLA, *Profili problematici in tema di documenti dichiarativi*, in *Ind. pen.*, 2008, vol. 11, fasc. 1, p. 106; V. PERCHINUNNO, *Prova documentale: b) diritto processuale penale*, in *Enc. dir.*, XXXVII, Milano, 1988, p. 722; P.P. RIVELLO, *La struttura, la documentazione e la traduzione degli atti*, in G. UBERTIS e M.G. VOENA (a cura di), *Trattato di procedura penale*, X.1, Milano, p. 24.

[45] Per un approfondimento, anche in chiave storica, del passaggio dal vecchio al nuovo codice, v. P. TONINI, *Manuale di procedura penale*, cit., pp. 28 e ss.

[46] Così, F. ZACCHÉ, *La prova documentale*, in *Trattato di procedura penale*, (diretto da) G. UBERTIS - G. P. VOENA, XIX ed., Milano, 2012, pp. 12 e 13.

[47] La cui massima espressione, come noto, è rappresentata dal "verbale". Cfr. P. TONINI, *Manuale di procedura penale*, cit., p. 183.

ed alle contestazioni (artt. 433, 511-514 c.p.p.)[48]. A livello legislativo, dunque, è netta la distinzione di disciplina tra entità materiali che, in quanto diverse, devono essere trattate giuridicamente in maniera differente. In particolare, «le norme [di utilizzabilità] sui documenti sono state concepite e formulate con esclusivo riferimento ai documenti formati fuori del processo nel quale si chiede o si dispone che esse facciano ingresso»[49]. Quanto alla documentazione, salvo eccezioni la regola è l'inutilizzabilità degli atti compiuti nelle fasi antecedenti al giudizio[50].

Il meritorio intento di chiarezza terminologica e di riorganizzazione sistematica operato dal legislatore del codice del 1988, tuttavia, non è servito ad evitare interpretazioni devianti. Ciò in quanto, nella prassi, «il confine tra atti e documenti è un terreno infido e malsicuro»[51]. Chiamata a confrontarsi su tale tematica, infatti, la nostra giurisprudenza, anche di legittimità, non ha dimostrato di avere idee troppo precise: a codice vigente, infatti, in numerosi casi sono stati acquisiti *ex* art. 234 c.p.p. oggetti che, invero, sarebbero dovuti risultare estranei alla disciplina della prova documentale[52]. Tra questi, per la particolare incertezza cui hanno dato luogo, meritano di essere citati: le registrazioni di colloqui effettuate dal privato, il quale partecipa alla conversazione, d'intesa con la polizia giudiziaria[53]; le registrazioni effettuate

---

[48] Con le seguenti precisazioni: i verbali di prova provenienti da altri procedimenti, così come le sentenze pronunciate in altri procedimenti penali, sono qualificabili come "prove extracostituite", disciplinate, rispettivamente, dagli artt. 238 e 238-*bis* c.p.p.: «L'effetto è singolare: i verbali concernenti prove "sono atti […] per il procedimento nel corso del quale si svolge l'assunzione probatoria, ma documenti […] per ogni altro processo in cui gli stessi vengano acquisiti"». Così, F. ZACCHÉ, *La prova documentale*, cit., pp. 13 e ss.; cfr., inoltre, G. UBERTIS, *Documenti e oralità nel nuovo processo*, in M.C. BASSIOUNI - A.R. LA TAGLIATA - A.M. STILE (a cura di), *Studi in onore di Giuliano Vassalli*, II, Milano, 1991, p. 119, il quale precisa che «risulta impossibile definire una volta per tutte se un certo documento sia 'processuale' od 'extraprocessuale', dato appunto che il discrimine tra i due gruppi concettuali si fonda non tanto sulle caratteristiche proprie dell'entità materiale volta a volta considerata quanto sulla relazione che viene instaurata tra essa ed il procedimento in cui se ne fa uso». Sull'art. 238-*bis* c.p.p., cfr., in particolare, L. IAFISCO, *la sentenza penale come mezzo di prova*, Torino, 2002, pp. 43 e 44.

[49] Cfr. *Relazione preliminare al c.p.p.*, Gazzetta Ufficiale, supplemento n. 2 del 24 ottobre 1988, p. 67.

[50] Cfr. art. 512 c.p.p.

[51] Così, A. CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove 'incostituzionali'*, in *Cass. pen.*, 1999, p. 1195.

[52] F. ZACCHÉ, *La prova documentale*, cit., p. 14, il quale aggiunge che la confusione è 'bilaterale': «per una vicenda […] dove un documento extraprocessuale (la registrazione d'un colloquio tra privati) è stato considerato alla stregua di un atto, cfr. Cass., sez. I, 10 ottobre 1995, Di Fiore, in *Cass. pen.*¸1996, p. 1183-1184, m. 662, con motivazione».

[53]Cfr. Cass., sez. II, 24 febbraio 2010, Caldaras, in *Giur. it.*, 2010, p. 1691; Cass., sez. VI, 24 febbraio 2009, Abis, in *Arch. n. proc. pen.*, 2010, p. 239; Cass., sez. III, 11 novembre 2008, in *Giur. it.*, 2009, p. 2772; Cass., sez. IV, 4 ottobre 2007, Picillo, in *Riv. pen.*, 2008, p. 837; Cass., sez. VI, 9 febbraio 2005, Rosi, in *Riv. pen.*, 2006, p. 363; Cass., sez. IV, 11 giugno 1998, Cabrini, in *Arch. n. proc. pen.*, 1999, p. 87; Cass., sez. I, 22 aprile 1992, Artuso, in *Cass. pen.*, 1993, p. 2588. *Contra*, tuttavia, cfr. Cass., sez. VI, 7 aprile 2010, Angelini, in *Foro it.*, 2011, II, p. 224; Cass., sez. un., 28 maggio 2003, Torcasio, in *Cass. pen.*, 2004, pp. 28 e 29; Cass., sez. I, 2 marzo 1999, Cavinato, in *Riv. pen.*, 1999, p. 1146; Cass., sez. I, 14 aprile 1999, Iacovone e altro, in *Riv. pen.*, 1999, p. 1037; Cass., sez. VI, 8 aprile 1999, Sacco e altri, in *Riv. pen.*, 2000, p. 188; Cass., sez. V, 10 novembre

direttamente dalla polizia giudiziaria, la quale partecipa fittiziamente alla conversazione[54]; le videoregistrazioni effettuate dalla polizia giudiziaria in occasione di attività investigative[55]; i disegni realizzati da un minorenne durante le sommarie informazioni[56].

E' necessario, quindi, fare chiarezza. Premessa della nostra riflessione è che il codice di procedura penale non contiene una definizione esplicita di documento[57]. Ciononostante, dall'art. 234, co. 1, c.p.p. e dalla sistematica del codice è possibile estrapolare almeno due requisiti fondamentali che devono sussistere affinché un determinato oggetto possa essere qualificato come documento in senso stretto: dal primo comma della prima norma dedicata alla prova documentale emerge il requisito positivo, ossia l'idoneità dello stesso a rappresentare un fatto, una persona o una cosa; dal sistema discerne, invece, il requisito negativo, ovvero la circostanza che l'elemento rappresentato debba costituire un *aliud* rispetto agli atti processuali compiuti nel procedimento all'interno del quale il documento è acquisito[58].

In altre parole, il documento esiste a prescindere dal procedimento penale; nasce in un momento[59] e per uno scopo del tutto diverso da quello che caratterizza le indagini che ivi si

---

2008, Poli e altri, in *Arch. n. proc. pen.*, 1999, p. 438; Cass., sez. VI, 26 marzo 1997, Mariniello, in *Giust. pen.*, 1998, III, pp. 697 e 698; Cass., sez. VI, 10 aprile 1996, Bordon e altro, in *Arch. n. proc. pen.*, 1996, p. 932; Cass., sez. II, 8 aprile 1994, Giannola, in *Giust. pen.*, 1995, III, p. 67.

[54] Cfr. Cass., sez. IV, 11 giugno 2009, Calciano e altri, in *Arch. n. proc. pen.*, 2011, p. 122; Cass., sez. III, 13 giugno 2001, Vanacore, in *Cass. pen.*, 2002, p. 2424: Cass., sez. I, 6 maggio 1996, Scali, in *Cass. pen.*, 1997, p. 1433.

[55] Cass., sez. VI, 17 novembre 2009, Drovandi e altro, in *Guida dir.*, 2010, n. 11, pp. 90 e 91; Cass., sez. V, 20 ottobre 2004, Held e altri, in *Riv. pen.* 2006, p. 132; Cass., sez. VI, 10 dicembre 1997, Pani e altro, in *Giust. pen.*, 1999, III, p. 238; Cass., sez. V, 25 marzo 1997, Lomuscio, in *Giust. pen.*, 1998, III, p. 313; Inoltre, cfr. Cass, sez. I, 10 luglio 2007, Susinni, in *Arch. n. proc. pen.*, 2008, pp. 491 e 492; Cass., sez. VI, 21 gennaio 2004, Flori, in *Riv. pen.*, 2005, p. 776; Cass., sez. IV, 18 giugno 2003, Kazazi, in *Riv. pen.*, 2004, p. 912; Cass., sez. VI, 10 novembre 1997, Greco, in *Cass. pen.*, 1999, pp. 1188 e 1189, le quali qualificano, in maniera terminologicamente contraddittoria, le vidoeregistrazioni realizzate dalla polizia giudiziaria come "prove documentali non disciplinate dalla legge", *ex* artt. 234 e 189 c.p.p.

[56] Cass., sez. III, 15 gennaio 2004, Sevà, in *Riv. pen.*, 2005, pp. 99 e 100.

[57] Limitandosi, *ex* art. 234, co. 1, c.p.p., a stabilire che «È consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo».

[58] Correttamente, quindi, la giurisprudenza di legittimità ha precisato che «ai fini dell'ammissione delle prove documentali sono necessarie due condizioni: a) che il documento risulti materialmente formato fuori, ma non necessariamente prima, del procedimento; b) che lo stesso oggetto della documentazione extraprocessuale appartenga al contesto del fatto oggetto della conoscenza giudiziale e non al contesto del procedimento». Così, Cass. pen., sez. 5, 16 marzo 1999, n. 6887, Gianferrari, rv. 213606; sez. 5, 16 marzo 1999, n. 5337, Di Marco, rv. 213183.

[59] Il documento si forma anteriormente o, comunque, al di fuori del procedimento in cui se ne chiede l'acquisizione. In dottrina, v. A. MARANDOLA, *I registri del pubblico ministero tra notizia di reato ed effetti procedimentali*, Padova, 2001, p. 1108-110; P. P. RIVELLO, *La struttura, la documentazione e la traduzione degli atti*, in G. UBERTIS - M.G. VOENA, (a cura di), *Trattato di procedura penale*, X.1, Milano, 2004, p. 19; G.P. VOENA, *Atti*, in *Compendio di procedura penale*, diretto da G. CONSO - V. GREVI, Padova, 2010, pp. 172 e 173. In giurisprudenza, cfr. Cass., sez. V, 13 aprile 1999, Gianferrari P., in *Riv. pen.*, 1999, p. 1145; Cass., sez. V, 16

svolgono; la sua utilità processuale è del tutto eventuale e dipende dalla sua qualificazione come cosa pertinente al reato o, addirittura, come corpo del reato[60].

La documentazione, invece, rappresenta la cristallizzazione di un'attività di indagine che intanto viene svolta in quanto esiste un procedimento penale all'interno del quale essa è realizzabile e potenzialmente utile, proceduralmente o processualmente, a seconda dei casi: si tratta del «risultato del comportamento tenuto da chi, nell'arco della sequenza procedimentale, svolga funzioni di decisione, d'accusa o di difesa: giudice, pubblico ministero, difensore e rispettivi ausiliari»[61]. Tale tipologia documentale nasce e muore con il procedimento penale in cui la relativa attività, documentata, viene realizzata.

Paradossalmente, il medesimo oggetto materiale, a seconda del modo e dello scopo per cui viene prodotto, può essere qualificato come documento o come documentazione: la ripresa video di un soggetto all'interno di un locale pubblico, se effettuata dalla polizia giudiziaria nel corso del procedimento penale in cui si indaga su quel soggetto, è documentazione, deve essere allegata al "verbale di operazioni (atipiche) compiute" e la sua ammissibilità nella fase dibattimentale passa attraverso l'art. 189 c.p.p., in quanto prova atipica; la stessa ripresa, se effettuata dallo stesso soggetto a scopo privato e poi rinvenuta e sequestrata dalla polizia giudiziaria nel corso di una perquisizione domiciliare, rappresenta un documento che entra nel processo a norma dell'art. 234 c.p.p.

Distinguere tra documento e documentazione non è puro esercizio accademico, fine a se stesso: dalla corretta qualificazione giuridica dipende il regime di utilizzabilità della prova. Ed allora, in presenza della rappresentazione di un fatto o di un atto diverso dall'atto processuale, siamo di fronte al "documento" in senso proprio[62], che, in quanto mezzo di prova, è di regola sempre utilizzabile in dibattimento[63]. Viceversa, quando la rappresentazione ha ad oggetto un atto o un'attività processuale, il codice utilizza il termine "documentazione"[64]: essa non è

---

marzo 1999, Di Marco, in *Riv. pen.*, pp. 1036 e 1037; Cass., sez. V, 12 novembre 1997, Dominici, in *Riv. pen.*, 1998, p. 158.

[60] V. F. ZACCHÉ, *La prova documentale*, cit., p. 37.

[61] Così, F. ZACCHÉ, *La prova documentale*, cit., p. 16. In dottrina, inoltre, v. P. TONINI, *Problemi insoluti della prova documentale*, in *Dir. pen. proc.*, 1996, p. 482, secondo il quale «per atto del procedimento si intende comunemente quell'atto che persegue le finalità del procedimento e che è compiuto da uno dei soggetti del procedimento», nonché A. CORBO, *I documenti*, in A. SCALFATI (a cura di), *Le prove*, in *Trattato di procedura penale*, II, diretto da G. SPANGHER, Torino, 2009, p. 325, dove si legge che «il sistema formato dagli artt. 511-514 c.p.p. disciplina l'acquisizione non di qualsiasi atto formato al di fuori del dibattimento, bensì - esclusivamente- di quegli atti che, oltre ad essere formati fuori del dibattimento, provengono da soggetti ai quali sono riconosciuti specifici poteri investigativi o di accertamento»

[62] Ad esempio, il diario di una persona.

[63] Cfr. Corte costituzionale n. 142 del 1992.

[64] La forma di documentazione di un atto del procedimento è, di regola, il verbale (cfr. art. 134 c.p.p.).

idonea a dar luogo ad un documento[65] e la sua utilizzabilità in giudizio dipende dalla disciplina giuridica del singolo atto di cui si tratta[66].

Più in particolare, tutto ciò che può essere qualificato come "documento" entra nel processo penale attraverso il mezzo di prova tipico disciplinato negli artt. 234 e ss. del codice di rito[67]: si tratta, infatti, di un elemento strutturalmente autonomo rispetto all'evolvere del procedimento penale, con una «genesi» che lo rende «insensibile a qualunque verifica circa il rispetto delle regole in materia di assunzione della prova, regole di cui il privato non è destinatario e che non operano oltre i confini processuali o, quanto alle indagini, oltre quelli procedimentali»[68]

Viceversa, quando il documento nasconde in realtà una documentazione, essendo la rappresentazione di un'attività svolta anche per interposta persona dall'accusa o dalla difesa, nell'ambito del medesimo procedimento penale in cui se ne vorrebbe l'acquisizione, esclusa in radice la possibilità di ricorrere alla normativa sulla prova precostituita, bisognerà «inquadrare la categoria in cui s'iscrive l'atto compiuto, per individuarne il regime d'utilizzabilità, una volta verificata la sua conformità rispetto al modello legale e ai relativi obblighi di documentazione»[69]. In altre parole, la documentazione necessita di uno strumento probatorio diverso e specifico per confluire legittimamente nel fascicolo del dibattimento ed il "canale di transito" dipenderà dal tipo di attività che viene svolta: la documentazione di atti tipici non ripetibili *ab origine* è utilizzabile a norma del combinato disposto degli artt. 431 e 357 c.p.p.; rispetto ad attività atipiche, l'unica norma fruibile appare invece l'art. 189 c.p.p.

Documento e documentazione sono, quindi, concetti da tener ben distinti e separati: la distanza che li separa è la stessa che divide la prova documentale dagli altri mezzi di prova e di ricerca della prova, tipici o atipici che siano[70].

---

[65] Salvo l'ipotesi in cui il verbale venga utilizzato in un differente procedimento penale. Cfr. art. 238 c.p.p.

[66] Ad esempio, gli atti di indagine sono, di regola, inutilizzabili in dibattimento.

[67] «[…] il documento confezionato da un privato -compresi imputato, persona offesa o danneggiato dal reato- in un contesto extraprocessuale verrà acquisito nei limiti di cui agli art. 234 e ss. c.p.p.». F. ZACCHÉ, *La prova documentale*, cit., p. 16.

[68] Cfr. Cass., sez. un., 28 maggio 2003, Torcasio, cit., pp. 28 e 29.

[69] F. ZACCHÉ, *La prova documentale*, cit., p. 17.

[70] In realtà, la distinzione concettuale tra la prova documentale dell'art. 234 c.p.p. e la prova atipica dell'art. 189 non è sempre stata chiara nemmeno nella giurisprudenza di legittimità. Con riferimento, in particolare, al tema delle "videoriprese", secondo un primo orientamento giurisprudenziale esse vanno incluse nella categoria dei documenti, posto che l'art. 234, innovando rispetto all'abrogato codice di rito, comprende in tale categoria le rappresentazioni di "fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo (In questo senso, Cass. pen., sez. 5^, 18 ottobre 1993, n. 10309, Fumero, rv. 195556; Cass. pen., sez. 3^, 15 giugno 1999, n. 11116, Finocchiaro, rv. 211457; Cass. pen., sez. 5^, 20 ottobre 2004, n. 46307, Held ed altri, rv. 230394). Secondo un diverso orientamento, invece, le riprese visive effettuate in luoghi pubblici devono

3. Sulla definizione giuridica di documento, dall'analogico al digitale

L'art. 234 del codice di rito definisce documenti gli «scritti» e gli «altri documenti che rappresent[i]no fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo»: «in un'unica categoria, dunque, sono state accorpate una serie di entità diverse, dagli scritti ai futuribili ritrovati tecnologici, il cui *trait d'union* è costituito dalla loro comune funzione rappresentativa»[71].

Etimologicamente, la parola documento deriva dal verbo *docere*, che significa insegnare, far conoscere[72], ed è definibile, per ora ed in via volutamente generica, come qualsiasi entità in grado di evocare qualcosa[73]. Trattasi, all'evidenza, di una entità «intenzionalmente rappresentativa di altro -giuridicamente rilevante- rispetto alla propria consistenza sensibile»[74]. In altre parole, per il mondo del diritto ciò che rileva è il contenuto rappresentativo[75] della *res* -la quale può essere del materiale più diverso[76]-, contenuto che rimanda ad un fatto rappresentato che, proprio in quanto incorporato nella *res*, "rivive" grazie a tale idoneità rappresentativa.

---

essere inquadrate nell'ambito delle prove atipiche, previste dall'art. 189 c.p.p., tanto se avvenute al di fuori del procedimento, quanto se avvenute nell'ambito delle indagini. Ciò in quanto il legislatore, disciplinando il documento come mezzo di prova, ha avuto di mira esclusivamente il documento precostituito e non il frutto di una ripresa visiva costituente mezzo di ricerca della prova. In questa prospettiva le riprese visive rappresenterebbero piuttosto una prova atipica, da acquisire con modalità che non si pongano in conflitto con norme di legge e, qualora venissero effettuate in un luogo pubblico o aperto al pubblico non incontrerebbero alcun limite, perché la natura del luogo in cui si svolge la condotta implicherebbe una implicita rinunzia alla riservatezza (Cfr. Cass. pen., sez. 4^, 16 marzo 2000, n. 7063, Viskovic, rv. 217688). Sul punto è intervenuta, nel 2006, la Corte di cassazione, nella sua composizione più autorevole, la quale ha avuto modo di chiarire che «solo le videoregistrazioni effettuate fuori dal procedimento possono essere introdotte nel processo come documenti e diventare quindi una prova documentale […], mentre le altre, effettuate nel corso delle indagini, costituiscono, secondo il codice, la documentazione dell'attività investigativa, e non documenti. Esse perciò sono suscettibili di utilizzazione processuale solo se sono riconducibili a un'altra categoria probatoria, che la giurisprudenza per le riprese in luoghi pubblici, aperti o esposti al pubblico, ha individuato in quella delle c.d. prove atipiche, previste dall'art. 189 c.p.p.» (Così, Cass., sez. un., 28 marzo 2006, Prisco, in *Dir. pen. proc.*, 2006, p. 1347).

[71] Così, F. ZACCHÈ, *La prova documentale*, cit., p. 20. Sulla rappresentazione, quale requisito caratterizzante il documento, cfr. *Relazioni al progetto preliminare e al testo definitivo del codice di procedura penale*, cit., p. 632, dove si legge che, una «volta definito il documento in ragione della sua attitudine a rappresentare, ne risulta una categoria unitaria i cui requisiti di utilizzabilità […] sono identici».

[72] F. CARNELUTTI, *Documento e negozio giuridico*, in *Riv. dir. proc. civ.*, 1926, I, p. 105.

[73] F. CORDERO, *sub. art. 234*, in *Codice di procedura penale commentato*, Torino, II ed., 1992, p. 280.

[74] Così, G. UBERTIS, *Documenti e oralità nel nuovo processo penale (1991)*, in ID., *Sisifo e Penelope. Il nuovo codice di procedura penale dal progetto preliminare alla ricostruzione del sistema*, Torino, 1993, p. 117.

[75] Sull'ampiezza del contenuto rappresentativo, cfr. F. CARNELUTTI, *Documento e negozio giuridico*, cit., p. 106; F. CORDERO, *sub art. 234*, cit., p. 280; R. D'ISA, *Sulla disciplina dei documenti nel nuovo processo penale*, in *Riv. it. dir. proc. pen.*, 1992, p. 1406; A. MALINVERNI, *Documento: b) diritto penale*, in *ED*, XIII, Milano 1964, p. 622.

[76] «Pietra, tavole cerate, carta, nastro magnetofonico, pellicola cinematografica o fotografica (in negativo o a stampa) e simili, sino alle odierne memorie informatiche o elettroniche». Così, F. ZACCHÉ, *La prova documentale*, cit., p. 8.

Da quanto appena esposto emerge la complessità del concetto giuridico di documento, correttamente definito come la «rappresentazione di un fatto che è incorporata su di una base materiale con un metodo analogico o digitale»[77]. Da tale definizione si ricavano i quattro elementi fondamentali che contribuiscono a dare consistenza al concetto di documento: il fatto rappresentato; la rappresentazione; l'incorporamento; la base materiale[78]. Il fatto rappresentato e la sua rappresentazione, entrambi giuridicamente rilevanti[79], sono diversamente "accessibili": il primo è un *lost fact*, ossia un accadimento appartenente al passato e irripetibile nella sua unicità; la seconda consente di rendere attuale quel fatto ricostruendolo, appunto, mediante rappresentazione. La ricostruzione del fatto, ossia la sua rappresentazione, viene quindi "fissata" su di una base materiale mediante un metodo di incorporamento. E' fondamentale comprendere appieno e distinguere bene tutti e quattro gli elementi citati, onde evitare inesattezze dalle pericolose conseguenze.

Il fatto rappresentato coincide con tutto ciò che può essere oggetto di prova[80]. E' oggetto di prova il fatto descritto nell'imputazione, nonché i fatti che consentono di quantificare la sanzione penale e quelli dai quali dipende l'applicazione di norme processuali[81]. Più in dettaglio, «può trattarsi non soltanto di un accadimento naturalistico […], ma anche di un atto umano, e quindi di una dichiarazione [di scienza o di volontà]»[82]. Così, il documento può raccontare di persone, cose o luoghi o rendere di nuovo presenti[83] avvenimenti naturali o umani verificatisi contestualmente o in un momento precedente alla sua formazione[84].

La rappresentazione di un fatto consiste nella sua attualizzazione mediante ricostruzione. In altre e più semplici parole, rappresentare un fatto significa ottenere oggi un equivalente (fatto noto) di ciò che è accaduto in passato (*lost fact*, ignoto)[85]. Tale opera di ricostruzione

---

[77] Cfr. P. TONINI, *Manuale di procedura penale*, cit., p. 356.
[78] *Ivi*, p. 362.
[79] «Al giurista non interessano i dati della vita reale in quanto tali» ma solo se suscettibili di considerazione «*sub* specie *iuris*». C. ANGELICI, *voce Documentazione e documento, in Enc. giur. Treccani*, XI, Roma, 1989, p. 1.
[80] *Ex* art. 187 c.p.p., infatti, per essere "pertinente" il documento deve necessariamente rappresentare un fatto oggetto di prova.
[81] Cfr. art. 187, co. 2, c.p.p.
[82] P. TONINI, *Manuale di procedura penale*, cit., p. 357.
[83] Da "*re-ad-praesentare*". Così, M. FERRARIS, *Documentalità. Perché è necessario lasciar tracce*, Roma, 2012, p. 24.
[84] Cfr. P. GUIDI, *Teoria giuridica del documento*, Milano, 1950, p. 36; F. CARNELUTTI, *La prova civile. Parte generale. Il concetto giuridico della prova*, Milano, rist. 1992, pp. 138 e 139; S. CAMPANELLA, *Profili problematici in tema di documenti dichiarativi*, in *Ind. pen.*, 2008, pp. 118 e 119; F. CORDERO, *Il procedimento probatorio*, in ID, *Tre studi sulle prove penali*, Milano, 1963, p. 12, nota 25.
[85] F. CORDERO, *Procedura penale*, Milano, 1971, p. 166.

fattuale può avvenire tramite parole, immagini, suoni o gesti[86]. La rappresentazione può avvenire per opera dell'uomo (testimonianza) o come risultato dell'utilizzo di uno strumento tecnico (apparecchio di registrazione).

L'incorporamento è la modalità attraverso la quale la rappresentazione del fatto viene fissata su di un supporto (base materiale) per essere conservata e successivamente fruita. Sono metodi di incorporamento, oltre alla tradizionale scrittura, la «fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo», purché, aggiungerei, idoneo a realizzare l'annessione tra la rappresentazione del fatto e la base materiale. La formula codicistica, volutamente aperta al progresso della tecnica, consente di distinguere due fondamentali categorie di metodi di incorporamento: quello analogico e quello digitale. Attraverso il metodo analogico[87], la rappresentazione viene incorporata sulla base materiale mediante grandezze fisiche variabili con continuità; in questo caso, l'incorporamento avviene "materialmente", nel senso che la rappresentazione non esiste senza il supporto fisico sul quale è incorporata. Attraverso il metodo digitale[88], invece, la rappresentazione viene incorporata sul supporto sfruttando grandezze fisiche variabili con discontinuità[89]. Nel fare ciò, la tecnica più utilizzata è il codice binario, una sequenza numerica di zeri e di uno[90]. Con una doverosa precisazione: anche il

---

[86] P. TONINI, *Manuale di procedura penale*, cit., p. 357.

[87] Con il termine "analogico" si fa riferimento a qualcosa di concreto, quindi visibile e/o tangibile. Il termine deriva da due parole greche, letteralmente traducibili in "discorso simile" o "parola uguale". Ciò che fa un sistema analogico infatti non è altro che imitare, rappresentare una quantità continuamente variabile attraverso un'altra quantità -analoga, appunto- nel modo più fedele possibile.

[88] "Digitale" deriva dal termine anglosassone *digit* che significa "cifra". Il concetto fa riferimento a qualcosa di astratto. Un sistema digitale sfrutta segnali discreti per rappresentare e riprodurre segnali continui sotto forma di numeri o altri caratteri.

[89] La differenza tra la tecnica analogica e quella digitale può ben essere esemplificata pensando agli orologi: per indicare il numero che rappresenta la misura del tempo corrente, gli orologi analogici usano delle grandezze variabili con continuità (gli angoli formati dalle lancette con un riferimento fisso), mentre gli orologi digitali usano una sequenza finita di simboli appartenenti ad un insieme finito (spesso le dieci cifre decimali ed i due punti). In sostanza, mentre nell'analogico il segnale varia con continuità, nel digitale il segnale assume un numero molto limitato di valori significativi diversi (si parla di segnale digitale o discreto).

[90] La tecnica binaria, che fa uso di due soli valori distinti, è di gran lunga la tecnica di memorizzazione digitale delle informazioni più utilizzata. Ciò sia grazie alla semplicità realizzativa dei circuiti che operano con due soli valori, sia al massimo livello di affidabilità che i segnali binari offrono. Prescindendo completamente dalla natura fisica dei segnali (due diversi livelli di tensione elettrica tra due morsetti o la presenza/assenza di corrente in un conduttore elettrico), nel codice binario si suole, per convenzione, indicare con i simboli "0" e "1" i due valori distinti utilizzati. A questi simboli si dà il nome di *bit* (da *binary digit).* Il *Bit* esprime l'alternativa tra 0 e 1 come minima unità d'informazione logicamente possibile. Un *bit* corrisponde alla quantità di informazione che otteniamo quando riceviamo una risposta a una domanda binaria, cioè a una domanda che ammette come risposta solo un "sì" o un "no" (nell'ipotesi che le due risposte abbiano la stessa probabilità). In altri termini, con un *bit* d'informazione possiamo rappresentare uno tra due possibili valori, come giorno/notte, sole/luna, accento/spento, falso/vero, 0/1, ecc. Con due *bit* possiamo rappresentare quattro valori differenti. In generale, con n*bit* possiamo rappresentare 2n di valori differenti. Il dato digitale che contiene l'informazione è composto da una sequenza di *bit*. Una sequenza di 8 *bit* viene detta *byte* e rappresenta la minima unità di informazione

digitale è un incorporamento di tipo materiale (che consiste, nel caso di *binary digit*, nella presenza o nell'assenza di un segnale elettrico, magnetico o luminoso[91]) su di un supporto fisico[92]. La differenza fondamentale tra le due modalità di incorporamento risiede nel fatto che, nel digitale, a differenza che nell'analogico, la rappresentazione esiste a prescindere dal supporto fisico sul quale è incorporata, nel senso che il dato informatico può essere trasferito agevolmente da un supporto all'altro senza perdere alcuna delle sue qualità[93]. In questo senso in dottrina il documento informatico è stato definito "dematerializzato" e non "immateriale"[94]: la fisicità del documento, seppur diversa, non manca; ciò che cambia è il suo legame con la base materiale. Si preferisce parlare di dematerialità, piuttosto che di immaterialità, perché, a ben guardare la reale differenza fra documento digitale e documento tradizionale non si gioca sul piano della materialità, quanto, piuttosto, sul diverso piano della autonomia o meno del contenuto informativo rispetto al supporto: nel documento tradizionale la "saldatura" tra informazione e supporto è reale, per cui esiste completa immedesimazione tra informazione e veicolo di tale informazione; nel documento informatico, invece, la "saldatura" è solamente ideale. Nel digitale, l'informazione -pur esistendo nella sua "materialità binaria", fatta di zeri e di uno - viene trasformata in impulsi elettronici: ciò rende accessibile il dato a prescindere dal supporto fisico prescelto per memorizzare quella specifica successione di *bit*.

---

gestibile da qualsiasi *computer*. Così S. ATERNO, *Acquisizione e analisi della prova informatica,* in *Dir. pen. proc.*, 2008, suppl. al n. 6, p. 62.

[91] Nel digitale, la materialità/fisicità dell'incorporamento risiede nella presenza/assenza di un segnale elettrico (nel caso di una *pen drive*), di un segnale luminoso (*cd* o *dvd*) o di un segnale magnetico (*hard disk*) su di un supporto fisico (la base materiale). Così, F. RICCI, *voce Documento informatico*, in *Il diritto, Enc. de Il Sole-24 Ore*, Milano, 2007, IV, p. 548.

[92] Cfr, da ultimo Cass. pen., sez. un., 29 gennaio 2015 (dep. 17 luglio 2015), n. 31022, Pres. Santacroce, Rel. Milo, reperibile al seguente url: www.penalecontemporaneo.it, in tema di sequestro di testate giornalistiche *on line*.

[93] Non rileva, invece, la necessità di avere la disponibilità di uno strumento tecnico al fine di cogliere l'essenza della rappresentazione: anche nel documento tradizionale, spesso, il contenuto rappresentativo non si può cogliere in assenza di apparecchiature adeguate. Quanto detto rappresenta, al tempo stesso, la croce e delizia del documento digitale: la gioia risiede nel fatto che tale tipo di documento può essere "trattato" per fini processuali e investigativi senza avere la necessità di sequestrare il supporto; il dolore deriva dalla facile alterabilità di tale documento, caratteristica imprescindibile della sua stessa essenza. Su quest'ultimo aspetto, tuttavia, appare opportuno fare un chiarimento: tutti i documenti sono potenzialmente a rischio di alterazione, ma solo nei documenti digitali una eventuale modifica (volontaria o accidentale che sia) è difficilmente dimostrabile *ex post.*

[94] Con riferimento al digitale, parla più correttamente di dematerializzazione e non di immaterialità P. TONINI, *Manuale di procedura penale*, cit., p. 358 secondo il quale, appunto, «è indifferente la base materiale sulla quale il documento informatico è fisicamente incorporato, purché ve ne sia una»; per tale motivo, non ci pare corretto affermare che l'incorporamento è "immateriale". E' immateriale l'opera dell'ingegno, la creazione dell'intelletto. Viceversa, l'incorporamento digitale avviene mediante la fissazione di un segnale elettrico, luminoso o magnetico su di una base materiale». In tale senso, cfr. anche F. ALCARO, *Riflessioni 'vecchie' e 'nuove' in tema di beni immateriali. Il diritto d'autore nell'era digitale*, in *Rass. dir. civ.*, 2006, p. 951.

La base materiale, infine, è il supporto sul quale è incorporata la rappresentazione del fatto. Essa può consistere nella carta tradizionale, nel nastro magnetico, nel più moderno supporto informatico. L'unico requisito richiesto per il supporto, vista la finalità probatoria del documento, è «l'idoneità a conservare la rappresentazione al fine di riprodurla quando occorra»[95].

Da quanto sino ad ora esposto emerge con chiarezza la differenza tra documento analogico, o tradizionale, e documento digitale, o informatico: il primo «può essere definito come quella rappresentazione di un fatto che è incorporata su di una base materiale con un metodo analogico» (uno scritto, una fotografia, un disco di vinile, ecc.); il secondo «può essere definito come quella rappresentazione di un fatto che è incorporata in una base materiale con un metodo digitale»[96].

Queste definizioni servono a fare chiarezza su un punto fondamentale, spesso trascurato anche in dottrina[97]: il documento informatico differisce rispetto al documento tradizionale unicamente sotto il profilo dell'incorporamento e mai per la rappresentazione, che rimane la stessa sia che si tratti di documento analogico sia che si tratti di documento digitale[98]. In altre parole, passando dal documento tradizionale al documento informatico, la variabile è il metodo di incorporamento, mentre la costante è la rappresentazione. Solo distinguendo correttamente tra i due elementi -rappresentazione e incorporamento- è possibile cogliere la differenza tra documento analogico e documento digitale.

Il documento informatico come elemento di prova[99] è unico[100], così come unica è la fonte di prova[101] da cui esso deriva. L'unicità deriva dalla "dematerializzazione"[102] del contenuto

---

[95] *Ivi*, p. 364.

[96] Così. P. TONINi, *Manuale di procedura penale*, cit., p. 358.

[97] Sulla base di una interpretazione letterale dell'art. 234 c.p.p., infatti, parte della dottrina ricava la conclusione che il documento è ogni cosa che rappresenta un fatto, una persona o un'altra cosa mediante la scrittura, la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo, considerando questi ultimi mezzi di rappresentazione anziché metodi di incorporamento. Lo stesso errore lo ha commesso il legislatore, nel codice dell'amministrazione digitale (d. lgs. 7 marzo 2005, n. 82), laddove si legge, *ex* art. 1, lett. p, che il documento informatico è la «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti». In realtà, quella informatica non è una forma di rappresentazione, ma un metodo di incorporamento, al pari della scrittura e degli altri metodi sopra citati. Cfr. P. TONINI, *Manuale di procedura penale*, cit., p. 358, nota n. 186.

[98] Incorporamento e rappresentazione, come già chiarito, sono elementi sì parimenti indefettibili ai fini della ricostruzione del concetto giuridico di documento, ma nettamente diversi: la rappresentazione passa necessariamente attraverso le parole, le immagini, i suoni o i gesti, perché rappresentare un fatto significa costruirne uno equivalente, in modo da renderlo conoscibile quando non sia più presente; l'incorporamento, viceversa, si avvale della scrittura, della fotografia, della cinematografia e della fonografia, i quali, quindi, non sono mezzi di rappresentazione, ma metodi di incorporamento, al pari dello strumento digitale.

[99] "Elemento di prova" è l'informazione grezza tecnicamente ricavabile dalla fonte di prova, ma giuridicamente non ancora sottoposta al vaglio valutativo del giudice. "Elemento di prova digitale", quindi, è il file, cioè il dato dematerializzato contenuto all'interno del supporto

rappresentativo del documento digitale, conseguenza diretta di un metodo di incorporamento, quello digitale, che lega elemento e fonte di prova in maniera del tutto peculiare ed innovativa rispetto a quanto avviene con riferimento al documento analogico. Dal punto di vista giuridico, come vedremo, ciò si riflette inevitabilmente sulle modalità corrette attraverso le quali "trattare" il documento per fini processuali, modalità differenti a seconda che si tratti di documento analogico piuttosto che di documento informatico.

Ciò rappresenta, al tempo stesso, croce e delizia dello studio del documento digitale: la gioia risiede nel fatto che tale tipo di documento può essere "trattato" per fini processuali e investigativi senza avere la necessità di sequestrare l'intero supporto; il dolore deriva dalla facile alterabilità di tale documento, caratteristica imprescindibile della sua stessa essenza.

L'aspetto positivo si coglie nella possibilità di rispettare il principio di proporzionalità[103] tra esigenze investigative e diritti della persona coinvolta nell'accertamento: la fungibilità del supporto consente infatti di evitare sequestri generalizzati comprendenti, in maniera indiscriminata, interi apparati informatici[104].

L'aspetto negativo è la facile alterabilità. Tale caratteristica, non nuova rispetto alla prova materiale tradizionale, cresce esponenzialmente quando si gestisce una prova digitale con strumenti di *computer forensics* in ragione della ontologica natura volatile, alterabile e

---

[100] Parla di "unicità", F. M MOLINARI, *Questioni in tema di perquisizioni e sequestro di materiale informatico*, cit., p. 274.

[101] "Fonte di prova digitale" è il luogo rappresentato -alternativamente o cumulativamente- dal sistema informatico (supporto statico tipo computer, *tablet*, *smartphone*, ecc.) e dal sistema telematico (rete internet) presenti sulla *scena criminis* e dai quali possono essere tratte informazioni utili per ricostruire un fatto del passato. Con una precisazione: oggi, parlare di *scena criminis* informatica significa riferirsi non soltanto al tradizionale personal computer, ma anche e sempre di più a dispositivi mobili quali *smartphone*, *tablet*, ecc. La fonte di prova di tipo digitale sta assumendo, nel corso di questi ultimi anni, un'importanza sempre maggiore in ragione del fatto che anche il diritto, così come tutta la società che questo cerca di ordinare, si sta muovendo sempre di più verso la digitalizzazione: ciò significa che, anche nel corso di investigazioni correlate a reati tradizionali, vengono in essere, quasi sempre, aspetti tecnologici che coinvolgono la scienza informatica.

[102] Come già detto, è' indifferente la base materiale sulla quale il documento informatico è fisicamente incorporato, purché ve ne sia una); per tale motivo, non ci pare corretto affermare che l'incorporamento è "immateriale". E' immateriale l'opera dell'ingegno, la creazione dell'intelletto. Viceversa, l'incorporamento digitale avviene mediante la fissazione di un segnale elettrico, luminoso o magnetico su di una base materiale» In tale senso, cfr. anche F. ALCARO, *Riflessioni 'vecchie' e 'nuove' in tema di beni immateriali. Il diritto d'autore nell'era digitale*, cit., p. 951.

[103] Preso in prestito dal diritto amministrativo (il principio di proporzionalità costituisce una specificazione del principio di ragionevolezza e del principio di imparzialità), in materia penale può essere concepito come principio di giustizia, laddove stabilisce il dovere delle autorità di realizzare i propri obiettivi alle migliori condizioni possibili, imponendo ai cittadini il minor onere possibile.

[104] Tale prassi giurisprudenziale, ancor prima dell'entrata in vigore della legge 48 del 2008, è stata duramente stigmatizzata dalla dottrina e successivamente censurata anche dalla giurisprudenza di legittimità. In dottrina, cfr. M. MATTIUCCI - G. DELFINIS, *Forensics Computing*., in *Rass. Arma Carab.*, 2006, p. 62, nonché P. TONINI, *Nuovi profili processuali del documento informatico*, in *Scienza e processo penale: linee guida per l'acquisizione della prova scientifica*, a cura di L. DE CATALDO NEUBURGER, Padova, 2000, p. 436, nota 14.

falsificabile di quest'ultima[105]. Il documento informatico, infatti, proprio perché scindibile rispetto al supporto che lo contiene, può essere facilmente modificato o alterato, dolosamente o colposamente, sia da parte di colui che ha formato il dato, sia da parte di terze persone che entrano per qualsiasi ragione in contatto con l'elemento dematerializzato. Con una doverosa precisazione: tutti i documenti sono potenzialmente a rischio di alterazione, ma solo nei documenti digitali una eventuale modifica (volontaria o accidentale che sia) è difficilmente dimostrabile *ex post*.

Ed è proprio per tale motivo -la particolarità del metodo di incorporamento e non del metodo di rappresentazione- che diventa necessario avere una disciplina *ad hoc* del documento informatico. Di tale necessità si è fatta carico la legge 18 marzo 2008, n. 48 (di esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica), la quale ha imposto una serie di cautele che assicurino la genuinità, la conservazione e la non alterazione del documento informatico "trattato" per fini processuali. Il punto sarà trattato successivamente nel capitolo dedicato alla prova informatica *off line*[106].

4. Prova scientifica e processo penale

Il metodo di incorporamento digitale che caratterizza e consente di distinguere il documento informatico dal documento analogico fa del primo una vera e propria prova scientifica[107]. Tale affermazione, se non precisata, rischia di ingenerare confusione.

La scienza non è in grado di far scalare ipotetiche classifiche in una ideale gerarchia delle prove del processo penale. La prova scientifica non è né prova regina, né prova debole[108], è soltanto una prova che deve calarsi all'interno del processo penale e seguirne le regole di

---

[105] Cfr. E. CASEY, *Error, uncertainty, and loss in digital evidence*, in *Int. J. Dig. Evidence*, 2002, p. 1.
[106] V. *infra*, Cap. II.
[107] Scientifica «è quel tipo di conoscenza che ha le seguenti caratteristiche: ha per oggetto i fatti della natura; è ordinata secondo un insieme di regole generali che sono denominate leggi scientifiche e che sono collegate tra loro in modo sistematico; accoglie un metodo controllabile dagli studiosi nella formulazione delle regole, nella verifica e nella falsificabilità delle stesse». Così, P. TONINI, *Progresso tecnologico, prova scientifica e contraddittorio*, in *La prova scientifica nel processo penale*, a cura di L. DE CATALDO NEUBURGER, Padova, 2007, pp. 49 e ss. Cfr., da ultimo, P. FELICIONI, voce *Prova scientifica*, in *Dig. mat. pen.*, VIII Agg., Torino, 2014, secondo la quale quattro sono i determinanti il crescente ricorso alla prova scientifica nella prassi: l'ampliamento del campo di applicazione di talune scienze; la sempre maggior attenzione dedicata all'accertamento del nesso causale; lo sviluppo di tecniche di indagine sempre più innovative; l'ingresso della scienza in «ambiti delicatissimi come la mente umana».
[108] *Contra*, cfr. G. PANSINI, *Le prove deboli nel processo penale italiano*, Torino, 2015.

valutazione. La prova scientifica non è una prova *sui generis*, impermeabile alle regole probatorie dettate nel codice di rito, ma deve «calarsi nei canoni della epistemologia processuale, nel rispetto tanto delle regole probatorie, quanto dei criteri di giudizio: dinamiche dello *ius probandi*, dell'onere della prova, del contraddittorio e del ragionevole dubbio»[109].

Dopo aver detto cosa la prova scientifica non è, proviamo a capire piuttosto in cosa consista: la prova scientifica è una categoria di genere, idonea a ricomprendere al suo interno tanto la prova critica o indiziaria, quanto la prova rappresentativa. La trasversalità della caratteristica scientifica della prova deriva dai diversi elementi della struttura probatoria sui quali è potenzialmente in grado di incidere la scienza: nella prova critica, la legge scientifica insiste sulla gravità dell'inferenza; nella prova rappresentativa, la scienza è in grado di influenzare l'attendibilità della rappresentazione o la credibilità della fonte (reale o personale che sia), confermandone o minandone l'idoneità rappresentativa.

Ovviamente, tutte le volte in cui è necessario operare una inferenza siamo di fronte ad un ragionamento di tipo indiziario, *nulla quaestio*. Ma ciò non toglie che il risultato ultimo di tale deduzione possa costituire la base per una successiva attività ricostruttiva del fatto ignoto che si fondi su una prova di tipo rappresentativo. Quindi, la scienza, e la prova scientifica che ne è una diretta derivazione in campo forense, incide anche sulla valenza della prova rappresentativa.

Ebbene, nel documento informatico il metodo di incorporamento è tale per cui una non corretta applicazione della scienza informatica inficia irrimediabilmente la capacità rappresentativa del documento stesso, al punto da far venire meno la certezza processuale del suo contenuto[110].

Dal 2002[111] tra i giudici italiani è in atto un vero e proprio scontro frontale sul modo di concepire il rapporto tra prova scientifica e processo penale. Da una parte, coloro i quali, rimanendo ancorati al passato, ritengono che non è compito del giudice valutare la legge scientifica, né in generale, né nella sua applicazione pratica al caso concreto: simili valutazioni spettano allo scienziato, con la conseguenza che l'errore scientifico non è emendabile nel processo. Dall'altra parte, coloro i quali attribuiscono al giudice il compito precipuo di verificare se la legge scientifica è valida in generale e, poi, se in concreto vi siano

---

[109] P. TONINI – C. CONTI, *Il diritto delle prove penali*, cit., p. 355.
[110] Cfr, da ultimo, Cass., sez. V, 7 settembre 2015, n. 36080, Sollecito, in www.giurisprudenzapenale.com.
[111] Lo spartiacque, come noto, è rappresentato da Cass., sez. un., 10 luglio 2002, n. 30328, Franzese, in *Cass. pen.*, 2002, p. 3643.

fatti tali da far ritenere che gli effetti constatati possano essere ricondotti all'operare di differenti cause. Ovviamente, al giudice non è richiesta alcuna competenza scientifica particolare, che evidentemente non può e non deve possedere, ma solo ed esclusivamente una competenza di metodo: egli deve essere il "giudice dei criteri", dovendo valutare la "scientificità" di una determinata spiegazione causale sulla base di criteri oggettivi e razionali, da esporre in motivazione[112].

[112] Cfr. Caso *Daubert v. Merrell Dow Pharmaceutical inc.* (92, 102), 509 U.S. 579, 1993, trad. it. in *Riv. trim. dir. proc. civ.*, 1996, pp. 277 e ss., con nota di A. DONDI, *Paradigmi processuali ed "*expert witness testimony*" nel diritto statunitense*, ivi, pp. 261 e ss. L' "erede" italiana della sentenza della Suprema Corte degli Stati Uniti è senz'altro Cass., sez. IV, 17 settembre 2010, n. 43786, Cozzini, in *CED Cass.*, 2010, 248944.

CAPITOLO 2
ISPEZIONI, PERQUISIZIONI, SEQUESTRI, RILIEVI E ACCERTAMENTI TECNICI SU MATERIALE DIGITALE

Sommario: 1. Il quadro normativo di riferimento: la legge 18 marzo 2008, n. 48 - 2. Le *best practices* nelle investigazioni informatiche - 2.1 Riconoscimento e individuazione della fonte di prova - 2.2 Acquisizione dei dati - 2.3 Conservazione dell'evidenza digitale - 2.4 Analisi dei dati e presentazione dei risultati - 3. I mezzi di ricerca della prova di natura digitale: ispezioni, perquisizioni, sequestri - 3.1 Ispezione tradizionale e ispezione informatica - 3.2. La perquisizione informatica - 3.3. Il sequestro probatorio di dati digitali - 4. Indagini tecniche su materiale digitale - 4.1 Il superamento della tradizionale distinzione tra rilievi e accertamenti tecnici - 4.2 Rilievi e accertamenti urgenti su materiale digitale: per una corretta interpretazione della loro "necessarietà" - 4.3 Verso una disciplina giuridica unitaria del potere tecnico-investigativo - 5. La ripartizione dell'onere della prova digitale - 6. Violazione dei protocolli e conseguenze processuali - 6.1 Sulla irregolarità - 6.2 Sulla nullità - 6.3 Sulla inutilizzabilità - 6.3.1 Sulla inidoneità probatoria - 6.3.2 Sulla carenza di potere istruttorio - 7. Le acquisizioni digitali all'estero ai sensi del nuovo art. 234-*bis* c.p.p.

1. Il quadro normativo di riferimento: la legge 18 marzo 2008, n. 48

Sino al 4 aprile 2008[113] l'ispezione, la perquisizione, il sequestro e, più in generale, le investigazioni urgenti aventi ad oggetto evidenze digitali erano attività prive di una espressa regolamentazione positiva. Di conseguenza, nella prassi spesso venivano utilizzati metodi operativi poco "sensibili" rispetto alle caratteristiche intrinseche dell'elemento di prova di natura digitale. Ma anche quando, da ultimo, le metodologie utilizzate dalle Procure più virtuose tendevano ad allinearsi alle esortazioni provenienti dalla scienza, appariva quantomeno incongruo che la garanzia dell'attendibilità degli elementi di prova fosse lasciata al buon senso dell'autorità inquirente. Ne risultava frustrato il principio di legalità probatoria, di cui all'art. 111, co. 1, Cost.

---

[113] Il giorno successivo segna l'entrata in vigore della legge 18.3.2008, n. 48, di Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno, pubblicata nella Gazz. Uff. 4 aprile 2008, n. 80, S.O. Tra i primi commenti alla normativa, cfr.: L. LUPARIA, *La ratifica della Convenzione cybercrime del Consiglio d'Europa. Profili processuali*, cit., pp. 717 e ss.; P. TONINI, *Documento informatico e giusto processo*, cit., pp. 401 e ss.; L. PICOTTI, *Ratifica della Convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'internet*, 2008, pp. 437 e ss.; M.L. DI BITONTO – A. VITALE – A. MACRILLÒ – A. BARBIERI – E. FORLANI, *La ratifica della Convenzione del Consiglio d'Europa sul Cybercrime: profili processuali*, in *Diritto dell'internet*, 2008, p. 503; A. BARBIERI, *Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici (commento a l. 18 marzo 2008, n. 48)*, in *Diritto dell'internet*, 2008, pp. 516 e ss.

Finalmente, con la legge 18 marzo 2008, n. 48, di ratifica della Convenzione di Budapest del 2001, il nostro legislatore, pur in ritardo, è intervenuto sull'impianto codicistico originario introducendo una vera e propria disciplina *ad hoc* relativa al trattamento della c.d. "evidenza digitale". Lo scopo dichiarato è stato quello di allineare, in conformità agli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea, le norme del codice di rito alle *best practices* di derivazione scientifica[114]. La *ratio* è evidente: scongiurare prassi lassiste che pretendevano di adottare tecniche e strumenti probabilmente utili per assicurare elementi materiali anche con riferimento agli elementi digitali. Per fare ciò, il legislatore del 2008 ha puntato sul risultato più che sul metodo, evitando di tipizzare la migliore tecnica operativa[115], ma pretendendo il raggiungimento dello scopo non negoziabile della preservazione del dato originale. Come vedremo, il miglior modo per ottenere tale obiettivo è rappresentato dalla previa duplicazione del dato, a condizione che la copia sia conforme all'originale e immodificabile[116].

A livello sistematico, il legislatore è intervenuto sul titolo III del libro III, relativo ai mezzi di ricerca della prova, e sul titolo IV del libro V, dedicato alle indagini su iniziativa della polizia giudiziaria, introducendo un vero e proprio "protocollo d'azione" per l'approccio alla c.d. prova di natura digitale, sia in sede di ispezioni (art. 244 c.p.p.) e perquisizioni -ad iniziativa della polizia giudiziaria (art. 352 c.p.p.) o delegate dal pubblico ministero (art. 247 c.p.p.)[117]-, sia in sede di sequestro di dati informatici presso fornitori di servizi informatici,

---

[114] La suscettibilità del dato informatico ad essere alterato o modificato ha imposto al legislatore della Convenzione di Budapest e, di riflesso, a quello italiano, l'indicazione di specifiche modalità per cercare di garantire efficace tutela dell'integrità delle informazioni digitali. Così, S. ATERNO, *Modifiche al titolo III del libro terzo del codice di procedura penale*, cit., p. 195; cfr, inoltre, G. ZICCARDI, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in AA.Vv., *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime*, a cura di L. LUPÀRIA, Milano, 2009, pp. 165 e ss.

[115] Scelta condivisibile in ragione della fisiologica tendenza all'obsolescenza di metodi e tecniche in una materia, come quella informatica, dove il progresso tecnologico cresce a livello esponenziale.

[116] «Le diverse interpolazioni disseminate a tale fine nel codice di rito appaiono tutte legate da un *fil rouge* che origina dall'idea di preservare in sede investigativa la genuinità della prova digitale, come si evince dalla formulazione delle nome che, modificando gli aspetti statici (artt. 244 e 247 c.p.p.) ovvero dinamici (artt. 352 e 354 c.p.p.) delle ispezioni e delle perquisizioni, prescrivono per l'accesso ai dati informatici l'adozione di "misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione" (artt. 8 e 9 della l. 18 marzo 2008, n. 48)». Così, E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit., p. 135.

[117] *Ex* artt. 244, co. 2, 247, co. 1-*bis*, c.p.p. e 352, comma 1-*bis*, c.p.p., è necessario: 1) che vengano adottate misure tecniche; 2) che le misure tecniche adottate assicurino la conservazione dei dati originali; 3) che le misure tecniche adottate impediscano l'alterazione dei dati originali.

telematici e di telecomunicazioni, *ex* art. 254-*bis* c.p.p., o in occasione di accertamenti urgenti, *ex* art. 354, co. 2, c.p.p.[118].

Probabilmente, la norma che maggiormente recepisce lo sforzo del legislatore del 2008 di tipizzare l'attività tecnica su materiale informatico durante la fase delle indagini preliminari è l'art. 354 del codice di rito, dedicata agli «accertamenti urgenti sui luoghi, sulle cose e sulle persone» ed all'eventuale «sequestro» ad iniziativa della polizia giudiziaria.

E' a tale soggetto processuale, dunque, che il legislatore si rivolge quando pretende che «in relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici» devono essere adottate «le misure tecniche» o «le prescrizioni necessarie ad assicurare la conservazione e ad impedire l'alterazione e l'accesso», sollecitando, «ove possibile», la «loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità»[119].

La garanzia fondamentale intorno alla quale ruota tutta la disciplina relativa al trattamento dell'evidenza digitale è rappresentata dal "dovere di non alterare il dato originale": le tecniche utilizzate per gestire gli elementi digitali devono essere in grado di lasciare inalterato l'originale, sia nella fase di acquisizione, sia nella fase successiva di conservazione[120]. Il miglior modo per raggiungere tale scopo è lavorare sulla copia, evitando in tal modo qualsiasi manipolazione degli elementi digitali originali. In altre parole, il legislatore, allineandosi alla migliore scienza ed esperienza del settore, ha recepito l'idea che qualsiasi tipo di "trattamento" del dato digitale ne compromette fisiologicamente l'integrità, in termini di dati e informazioni da esso estrapolabili. Quindi, il modo più corretto di procedere per garantire la non alterabilità dell'originale consiste nel farne una "copia" per poter "lavorare" su quest'ultima[121]. Ovviamente, rispetto a tale copia l'investigatore deve offrire idonee garanzie di "genuinità" e di "conservazione". Tali concetti, seppur spesso trattati allo stesso modo, non sono sinonimi: garantire la genuinità significa assicurare l'esatta corrispondenza tra la copia e l'originale nel

---

[118] *Ex* art. 354 c.p.p.: 1) l'acquisizione, «ove possibile», deve avvenire mediante copia dei dati; 2) la copia dei dati informatici deve essere effettuata su adeguato supporto; 3) la procedura di acquisizione deve essere condivisa e controllabile; 4) la procedura scelta deve essere tale da assicurare l'immodificabilità dei dati copiati; 5) i dati originali devono comunque essere conservati e protetti adeguatamente.

[119] In sintesi, nel trattamento dell'evidenza digitale l'operatore deve osservare: «1) il dovere di conservare inalterato il dato informatico nella sua genuinità; 2) il dovere di impedire l'alterazione successiva del dato digitale; 3) il dovere di formare una copia che assicuri la conformità del dato informatico acquisito rispetto a quello originale; 4) il dovere di assicurare la non modificabilità della copia del documento informatico; 5) la garanzia dell'installazione di sigilli informatici sui documenti acquisiti». Così, P. TONINI, *Manuale di procedura penale*, cit., pp. 378-379.

[120] Si tratta delle «prescrizioni necessarie ad assicurare la conservazione e ad impedire l'alterazione e l'accesso».

[121] Ecco perché è caldeggiata «l'immediata duplicazione su adeguati supporti».

momento stesso in cui viene realizzata la copia forense[122]; conservare del dato, invece, significa impedire alterazioni successive della copia stessa[123].

Ciò premesso, il nodo problematico da sciogliere consiste essenzialmente nella corretta qualificazione giuridica dell'attività tecnica finalizzata alla c.d. "copia forense" dei dati. Copiare, infatti, significa comunque "intervenire" sul dato originale, ma, come detto in premessa, qualsiasi tipo di "trattamento" -e quello finalizzato alla copia non sfugge a questa logica- rischia di compromettere l'integrità del dato. Ergo, dalle modalità tecniche del suo svolgimento e dal contesto operativo contingente dipendono il suo corretto inquadramento giuridico.

Posto che con riferimento alla realtà dematerializzata l'urgenza è in *re ipsa,* derivando fisiologicamente dalla volatilità e dalla labilità del dato digitale[124], la questione da dirimere per individuare la disciplina applicabile all'attività tecnica di copia riguarda, più che altro, la ripetibilità o meno dell'attività medesima, che a sua volta dipende dalla potenziale alterabilità dell'elemento digitale oggetto di accertamento.

La *sedes materiae* per fare spazio, all'interno del codice di rito, alla prova di natura digitale è stata individuata nelle norme dedicate agli atti a sorpresa e in quelle che disciplinano l'attività urgente -in quanto non differibile- della polizia giudiziaria, attività entrambe fisiologicamente incompatibili con una garanzia partecipativa che preveda un contraddittorio anticipato con la controparte.

In particolare, con riferimento alla realtà dematerializzata il legislatore interviene sull' "effetto sorpresa" e sull' "urgenza", coniugandoli con la "ponderazione": impellenza e meditazione, solitamente concetti antitetici in qualsiasi tipo di attività umana, devono necessariamente convivere nel processo penale quando si parla di indagini informatiche aventi ad oggetto elementi di prova di natura digitale[125]. Tale convivenza è necessaria per garantire, prima ancora che il diritto di difesa in termini di garanzia del contraddittorio (quantomeno

---

[122] Come vedremo, tale garanzia è oggi offerta dalla c.d. *bit stream immage*, "sigillata" attraverso un algoritmo di *hash*.

[123] Attraverso, ad esempio, dei software di *write blocking*.

[124] Sicché, con esclusivo riferimento alla "copia forense", difficilmente praticabile appare il ricorso all'istituto dell'incidente probatorio, così come l'esercizio di poteri tecnici unilaterali differiti sul materiale digitale.

[125] «L'urgenza, dunque, esige meditazione, in ottemperanza a un monito *prima facie* dissonante che *in subiecta materia* doppiamente si impone, involgendo il momento pratico di concreta operatività dell'esplorazione informatica non dilazionabile e, prima ancora, la dimensione teorica del suo astratto inquadramento». Così, E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit., p, 136.

postumo) e di parità delle armi, anche e soprattutto l'attendibilità oggettiva dell'accertamento finalizzato a determinare una eventuale responsabilità penale[126].

Ma cosa significa, processualmente, far convivere "urgenza" e "ponderazione"? Come è possibile conciliare l'impellenza dell'accertamento unilaterale con la meditazione e la riflessione? Tradotto in diritto delle prove nel processo penale, ciò significa sostanzialmente inutilizzabilità[127] delle evidenze digitali unilateralmente raccolte, stante l'urgenza, con metodi inidonei a garantire la conservazione del dato originale o, comunque, inadatti ad essere verificati *ex post* dalla controparte.

Due, quindi, i requisiti fondamentali che devono caratterizzare l'attività indifferibile su dati informatici: 1) idoneità del metodo utilizzato a garantire la preservazione dei dati originali; 2) idoneità del metodo ad essere sottoposto a controllo, quanto meno differito[128].

Entrambi i requisiti sono indefettibili, nel senso che la mancanza di uno solo di essi dovrebbe avere come conseguenza l'esclusione dell'evidenza digitale dal panorama conoscitivo legittimamente attingibile da parte del giudice[129]: il primo requisito rappresenta la migliore garanzia, dal punto di vista oggettivo, di un accertamento attendibile; il secondo, invece, rappresenta l'attuazione, dal punto di vista soggettivo, del principio del contraddittorio nella formazione della prova, nel suo nucleo insopprimibile di garanzia della possibilità di verificare, quantomeno successivamente, l'operato della controparte[130].

L'investigazione digitale non procrastinabile non sfugge a questa logica: «al contrario, sono proprio le incombenze indifferibili a esigere la massima conformazione ai principi enunciati poiché la concitazione del momento può favorire prassi lassiste motivate dalla

---

[126] D'altronde, «è proprio un'esplicita esortazione alla prudenza investigativa ad animare lo spirito complessivo del recente intervento di riforma attuato, anche sul versante processuale, per adeguare le norme interne alle peculiarità dello strumento digitale», *ivi*, p. 135.

[127] Sulle diverse opinioni riguardo alle "conseguenze processuali", cfr., *infra*, par. 7, in questo capitolo.

[128] Tale approdo ermeneutico deriva dalla tradizione giuridica di *common law*, a cui si deve la distinzione tra *intrinsic policy* ed *extrinsic policy* per indicare le regole di esclusione probatoria finalizzate a proteggere, rispettivamente, l'affidabilità dei risultati conoscitivi e il diritto di difesa. Cfr. L. LUPARIA, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, p. 142.

[129] «Il nodo interpretativo scivola sulle questioni inerenti alle metodiche operative e alla possibilità di una loro successiva verifica. Invero, soltanto ove l'azione si uniformi a canoni condivisi, idonei ad assicurare la corretta preservazione del dato digitale ed *ex post* controllabili, sarà possibile annoverarla tra le autentiche rilevazioni indifferibili suscettibili di compimento unilaterale (artt. 354, comma 2, secondo periodo, 359 e 391-*sexies* c.p.p.). Per converso, allorché l'azione segua protocolli inadeguati a garantire l'integrità della risultanza ovvero non passibili di successiva verifica, dovrà concludersi che con la rilevazione è stata compiuta un'irreversibile modifica dell'oggetto digitale, il quale ultimo potrà essere preso in considerazione soltanto ove assistito, nella fase di originaria captazione, del contraddittorio preventivo prescritto dall'art. 360 c.p.p.». Così, E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit., p. 148.

[130] Cfr., P. TONINI, *Il documento informatico: problematiche civilistiche e penalistiche a confronto*, cit., p. 435.

premura dell'agire, tanto più insidiose nel frangente di primo contatto con la fonte di prova capace di condizionarne la capacità euristica *ab imis* e *sine die*"[131]. Non a caso, la procedimentalizzazione dell'indagine informatica effettuata con gli innesti del 2008 ha cercato di porre un freno a «pratiche devianti che il costume investigativo aveva fatto registrare in assenza di una disciplina puntuale di protocolli operativi garanti di attendibilità e contraddittorio»[132].

Con la seguente precisazione, prima di procedere: quando si parla di indagini informatiche ciò che rileva ai fini della applicabilità di una o dell'altra disciplina è l'elemento oggettivo e mai quello soggettivo. Ciò significa che l'obiettivo della conservazione e della genuinità è doveroso, sia per la polizia giudiziaria che per il pubblico ministero e per i difensori privati: pur nel silenzio del legislatore[133], infatti, una simile interpretazione estensiva si rende necessaria per evitare irragionevoli disparità di trattamento, censurabili *ex* art. 3 Cost., tra investigatori che dovrebbero muoversi su un piano di parità nella rigorose maglie che caratterizzano le regole probatorie nel procedimento penale. D'altronde, la *ratio* della novella è quella di garantire *standard operating procedures* in occasione del compimento di indagini su elementi digitali, a prescindere dal soggetto che le ponga in essere: «trattasi […] di norme precauzionali di buona condotta investigativa che si riflettono sulla successiva utilizzabilità della risultanza digitale sì da imporsi come decalogo operativo per ciascun investigatore 'urgente' di *computer forensics*»[134].

2. Le *best practices* nelle investigazioni informatiche

Come abbiamo già avuto modo di sottolineare, due sono i requisiti fondamentali che devono caratterizzare l'attività indifferibile su dati informatici: 1) attendibilità del metodo di "trattamento"; 2) idoneità del metodo ad essere sottoposto a controllo, quanto meno differito. L'attendibilità dell'evidenza digitale nel processo penale dipende da una garanzia complessa che copra tanto l'originale, in termini di "conservazione", quanto la copia del dato, in punto di

---

[131] Così, E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit., p. 138. Su questo aspetto, insiste, inoltre, G. ZICCARDI, *Le tecniche informatico-giuridiche di investigazione digitale*, cit., p. 52.
[132] E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit., p. 138.
[133] Con riferimento alle indagini, la legge n. 48 del 2008 non ha interessato gli artt. 359, 360 e 391-*sexies* c.p.p., ma solo gli artt. 352 e 354 c.p.p.
[134] E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit., p. 150.

"genuinità" e di "non modificabilità". La verificabilità del metodo dipende dalla intelligibilità della procedura di acquisizione del dato digitale.

Tali risultati possono essere raggiunti attraverso un preciso protocollo che deriva dalle migliori metodologie (*best practices*) invalse nella prassi investigativa internazionale[135]. Si tratta di linee guida[136] che hanno come obiettivo comune la prevenzione dal rischio di inquinamento della risultanza digitale. La scienza che si occupa della implementazione di tali protocolli è nota con il nome di *digital forensics*[137]. Dalla maturata consapevolezza della esponenziale crescita di importanza di tale scienza nel processo penale deriva la necessità di un approfondimento, anche tecnico, di tale disciplina[138]. Occorre dunque uno sforzo per

---

[135] A livello europeo, esistono delle linee guida per l'identificazione e la gestione delle fonti di prova digitale. Si tratta di norme di *soft law* che rappresentano la traduzione operativa delle generiche formule adoperate a livello legislativo per garantire l'autenticità della prova digitale nel processo penale. Questo manuale per addetti ai lavori (*Electronic Evidence Guide*), frutto di un progetto finanziato dal *Council of Europe* e dall'Unione Europea conclusosi nel marzo del 2013, è disponibile gratuitamente al seguente url: www.coe.int/cybercrime. La traduzione italiana, nata dallo sforzo congiunto delle associazioni *Digital Forensics Alumni, Tech and Law Center e DEFT Association*, è scaricabile gratuitamente compilando il *form online* disponibile al seguente indirizzo: http://bit.ly/eeg-ita-form. A livello internazionale, invece, cfr. la norma ISO/IEC 27037:2012 in tema di identificazione, raccolta, acquisizione e conservazione delle prove digitali (consultabile al seguente sito: www.iso.org).

[136] Con il termine "linee guida" si fa riferimento ad un insieme di raccomandazioni sviluppate sistematicamente, sulla base di conoscenze continuamente aggiornate e valide, redatto allo scopo di rendere appropriato, e con un elevato standard di qualità, un comportamento desiderato. E' indubbio che le linee guida costituiscono la base di partenza per l'impostazione di comportamenti e modus operandi condivisi in organizzazioni di ogni genere (sia private, sia pubbliche) nel campo sociale, politico, economico, aziendale, medico e, di recente, giuridico. Indicativo in questo senso il ruolo ed il valore delle linee guida descritto dalla Suprema Corte in relazione all'attività medico chirurgica, allorché si è precisato che esse «costituiscono sapere scientifico e tecnologico codificato, metabolizzato, reso disponibile in forma condensata, in modo che possa costituire un'utile guida per orientare agevolmente, in modo efficiente ed appropriato, le decisioni terapeutiche» ed attraverso il quale «si tenta di oggettivare, uniformare le valutazioni e le determinazioni e di sottrarle all'incontrollato soggettivismo del terapeuta». Così, Cass., Sez. 4, nr. 16237 del 29/01/2013 (dep. 09/04/2013), Cantore, Rv. 255105.

[137] Appare opportuno distinguere tra *digital forensics, computer forensics, network forensics, mobile forensics e PDA o SIM forensics*: la prima ha ad oggetto, in generale, il dato digitale ovunque esso si trovi; la computer forensics si occupa specificatamente di personal computer, fissi o portatili, e di tutte le periferiche di archiviazione di massa con essi utilizzabili; si parla, invece, di mobile forensics per indicare l'analisi dei dispositivi mobili idonei all'elaborazione informatica di dati e informazioni. Inoltre, è necessario tener ben presente la differenza tra "informatica forense" e "sicurezza informatica": quest'ultima studia ed implementa tecniche e protocolli finalizzati a rendere il più possibile sicuro un determinato sistema informatico da attacchi esterni ; la prima, invece, oggetto del presente paragrafo, studia ed implementa procedure tese a fornire adeguate garanzie in termini di integrità, autenticità e disponibilità di dati e informazioni di natura digitale, in vista di un loro potenziale utilizzo in chiave processuale. Fatto tale distinguo, appare chiaro che la scienza etichettata con il nome di "informatica forense", lungi dal limitare il proprio raggio d'azione alle sole indagini relative ai c.d. reati informatici, esplica la sua importanza, oggi, con riferimento a qualsiasi tipologia di illecito penale, dai reati informatici puri, sino ai reati tradizionali: un qualsiasi utente, operando su di un sistema di elaborazione, crea, spesso a sua completa insaputa, tracce che possono divenire prove di un'attività illecita.

[138] Le garanzie codicistiche introdotte dalla novella del 2008 individuano tacitamente la *computer forensics* quale ausilio tecnico indispensabile degli inquirenti. Cfr. F. NOVARIO, *Criminalità informatica e sequestro probatorio: le modifiche introdotte dalla l. 18 marzo 2008, n. 48 al codice di procedura penale*, in *Riv. dir. proc.*, 2008, p. 1070. Per un approfondimento sul collegamento implicito, ma inequivocabile, tra la prova informatica e la scienza nota come *computer forensics*, cfr. S. ATERNO, *Acquisizione e analisi della prova informatica*, cit., pp.

mantenere alto il livello di aggiornamento e la specificità di conoscenze e di competenze della tecnologia informatica, al fine di far rivivere in concreto i principi nella dimensione specifica che oggi devono assumere.

La *digital forensics*, o scienza delle investigazioni digitali o, ancora, informatica forense, è la disciplina che studia, in generale, il "trattamento" del dato digitale per fini processuali. Quale "scienza forense" essa studia le modalità più opportune per salvaguardare il "valore processuale" di determinati accadimenti, al fine precipuo di far assurgere la rappresentazione di tali fatti al rango di "prove"[139]. La peculiarità di tale scienza risiede nel fatto che i fatti e gli elementi oggetto di studio sono i dati digitali.

Nell'ambito di un'attività investigativa finalizzata alla assicurazione di fonti di prova di natura digitale si rende necessaria l'esecuzione delle seguenti macro-attività: a) individuazione e riconoscimento della fonte di prova; b) acquisizione dei dati; c) conservazione dei dati; d) analisi forense e presentazione dei risultati.

2.1 Riconoscimento e individuazione della fonte di prova

Il primo *step* del *digital forenser* consiste nella esatta individuazione della fonte dell'evidenza digitale. Si tratta di un'attività di mera osservazione che non dovrebbe mai comportare un accesso tecnico al sistema informatico o telematico oggetto di interesse investigativo. Sostanzialmente, tale fase consiste nella mera constatazione dello *status quo* e, a livello operativo, si traduce nella osservazione preliminare delle condizioni in cui si presentano i dispositivi da esaminare, al fine di immortalare e documentare[140] lo stato dell'ambiente digitale prima dell'intervento dell'investigatore. Più in dettaglio, si tratta di verificare quali e quanti sono i dispositivi da "trattare", come sono collegati fra loro, se esista un collegamento Internet attivo o una rete interna, ecc. La *scena criminis* digitale, inoltre, deve essere delimitata: è necessario quindi individuare i supporti di memorizzazione digitale di interesse investigativo, scartando quelli ritenuti superflui. Questa attività può non essere

---

61 e ss., nonché S. ATERNO, *Digital forensics (investigazioni informatiche)*, in *Dig. disc. pen. (agg.)*, 2014, p. 217-247.

[139] Non bisogna mai perdere di vista il fine di tale attività tecnica di indagine: si tratta di una scienza forense, come tale orientata alla individuazione di regole e principi da applicare in concreto per il corretto trattamento del dato digitale per un fine ben preciso, che è quello della sua valutazione come prova nel processo.

[140] Attraverso verbalizzazione e, se possibile, videoripresa dell'ambiente in cui si andrà successivamente ad intervenire.

così semplice e scontata come appare[141]: il dato dematerializzato, infatti, può essere contenuto in diverse tipologie di supporti, come *hard disks*, media rimuovibili, oppure può consistere in un *file* di *log* su un *server*. Per ciascuno dei supporti individuati è necessario predisporre un "ordine di volatilità" (*order of volatility*) e cioè capire quali sono i dati che devono essere acquisiti prima degli altri per evitarne la cancellazione o la sovrascrittura con altri dati. In particolare, si deve procedere dal dato più volatile a quello più persistente[142].

Evidentemente, le difficoltà di una corretta individuazione dell'evidenza digitale aumentano in maniera inversamente proporzionale rispetto alle competenze tecniche e all'esperienza degli operatori che compiono il sopralluogo.

2.2 Acquisizione dei dati

Il secondo *step*, sicuramente il più delicato di tutto il processo di *computer forensic*, consiste nell'acquisizione genuina degli elementi di prova digitale. L'acquisizione della prova informatica è sicuramente la fase che presenta maggiori criticità, proprio perché deve garantire l'inalterabilità dell'elemento che viene ad essere repertato e la sua fissazione nel tempo. Tale procedura non potrà essere attuata come una mera "copia" del dato ricercato, poiché un'operazione di questo tipo comporterebbe, oltre all'irreparabile perdita dei c.d. metadati[143], anche la mancanza di un'esatta corrispondenza contenutistica tra dato originale e copia.

Dal punto di vista tecnico, l'integrità dei *files* originali può essere garantita attraverso la c.d. *bit stream image*, ovvero una copia-clone (*bit* a *bit*), *on site*, delle informazioni digitali. A differenza di un semplice *backup* dei dati, che si preoccupa di salvare su un supporto differente una copia dei dati presenti sul disco originale, una copia *bit* a *bit* è un duplicato esatto dell'intero supporto originale. Un'immagine *bit stream* è, quindi, un file che contiene una replica di tutti i dati contenuti su un disco o su una partizione di un disco, ivi compresi

---

[141] «In una realtà dove è difficile delimitare l'area geografica e logica del crimine, può diventare estremamente difficile discernere con precisione quali siano le possibili fonti di prova, quali le aree del sistema da analizzare, quali i dati da elaborare per primi, quali strumenti utilizzare per il *data mining* e per il filtraggio dei dati utili da quelli inutili o falsi o che possono creare confusione e ostacolare le indagini». Così, G. ZICCARDI, *Informatica giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni digitali*, Tomo II, Seconda ed., Milano, 2012, p. 265.

[142] Per fare un esempio, l'ordine di volatilità per un *personal computer* potrebbe essere il seguente: registri di sistema; memoria fisica e memoria virtuale; *routing table; arp cache;* tabella dei processi in esecuzione; *file system* temporanei; *hard disk;* configurazione fisica e topologia di rete; media di archiviazione e di backup (CD, DVD, NAS, ecc.).

[143] Ci si riferisce ad esempio alle indicazioni temporali di creazione del file, di sua modifica o di cancellazione.

files cancellati, definitivamente rimossi o nascosti. Per comprendere meglio il concetto di copia *bit stream*, si potrebbe astrattamente immaginare di poter leggere in maniera sequenziale tutti i bit memorizzati all'interno di un supporto e duplicarli, mantenendo inalterata la loro sequenza e collocazione fisica e logica all'interno di un nuovo dispositivo di memorizzazione, senza preoccuparsi di interpretarne il significato. Quindi, un'immagine *bit stream* altro non è se non il "clone" esatto del dispositivo o del supporto repertato.

Ovviamente, la copia forense dei dati da un dispositivo di memorizzazione digitale delle informazioni può essere realizzata con differenti modalità, a seconda della metodologia operativa seguita[144], del sistema operativo della macchina[145] e del software utilizzato per

---

[144] Dal punto di vista metodologico, il *computer forenser* ha due fondamentali possibilità: smontare il supporto di memorizzazione dal computer a cui si trova collegato (nella *scena criminis* originale) e collegarlo ad una macchina forense per l'acquisizione; acquisire l'immagine del disco utilizzando direttamente il computer oggetto di analisi come sorgente, salvando il risultato su un supporto esterno rimuovibile o su una macchina forense via rete

[145] In ambiente Linux, l'acquisizione dei dati si può realizzare utilizzando il comando nativo *dd*, oppure una sua variante con maggiori performance, ovvero *dcfldd*. Questi comandi possono realizzare una copia bit-a-bit di un intero hard disk in un file immagine, a partire da un qualsiasi disco che il sistema operativo sia in grado di interpretare (in particolare sono supportate le partizioni EXT2FS, EXT3FS, FAT12, FAT16, FAT32, NTFS, HFS e HPFS. Il vantaggio di questa soluzione è che è completamente gratuita, a condizione di una buona conoscenza e comprensione dei comandi di *shell* di un sistema operativo *Linux*). Per venire incontro alle esigenze di rapidità e di praticità di utilizzo sono state sviluppate alcune distribuzioni Live di Linux, che consentono l'avvio del computer da CD o da memoria USB esterna. Queste distribuzioni hanno il vantaggio di poter essere avviate direttamente sulla macchina oggetto di analisi (verificando, ovviamente, la sequenza di boot del personal computer) e consentono al *digital forenser* di individuare tutti i supporti di memorizzazione presenti nel personal computer e di accedervi in sola lettura. Una volta individuate le fonti di dato che si vogliono duplicare, sarà sufficiente collegare un dispositivo esterno o una connessione di rete su cui salvare l'immagine dell'hard disk. Per poter scrivere su un supporto esterno sarà necessario montare il dispositivo in modalità lettura e scrittura, tramite il comando nativo *mount* Le principali distribuzioni Live di Linux attualmente disponibili su web sono: *Helix 3 Enterprise*, sviluppato da *e-Fense*, *ex* progetto gratuito che ora prevede un abbonamento mensile; DEFT (*Digital Evidence & Forensic Toolkit*) *Linux*, sviluppato da Stefano Fratepietro; CAINE (*Computer Aided Investigative Environment*), sviluppato da Nanni Bassetti; *SMART Linux*, sviluppato da ASR Data; *Forlex*, sviluppato da Luca Guerrieri; *IRITALY Project* (*Incident Response Italy Project*), sviluppato da Dario Forte (questo progetto è in *End of Life* e non saranno disponibili nuove release); *The Penguin Sleuth Kit*, sviluppato da Ernest Baca; *Backtrack 4*, sviluppato come distribuzione per il *penetration testing* dispone di alcuni *tool* di *Computer Forensics*). Per sua natura, il sistema operativo Linux sembra essere il più indicato per una acquisizione dei dati in ottica forense poiché è in grado di rendere un hard disk accessibile solamente in lettura, garantendo a livello software una integrità e una non-scrittura sul supporto originale. In ogni caso, per minimizzare il rischio di alterazione, è consigliabile utilizzare dispositivi di *write blocking*, che impediscano a livello hardware la scrittura sul supporto originale. In ambiente Windows, invece, esistono diversi programmi applicativi che consentono la copia forense dei dati. Con una precisazione: per l'acquisizione sotto Windows non sono al momento disponibili Live CD con cui avviare il computer. È quindi necessario procedere allo smontaggio fisico dell'hard disk dal computer oggetto di analisi e al collegamento ad una macchina forense dedicata. Poiché il disco viene collegato ad un sistema operativo Windows è necessario, per garantire il blocco dell'accesso in scrittura, utilizzare un write blocker (hardware o software). I principali *tool* di acquisizione disponibili in ambiente Windows sono: *AccessData FTK (Forensic Toolkit) Imager*, *freeware* che consente di acquisire immagini di interi dispositivi fisici o di partizioni logiche (FAT, NTFS, EXT2, EXT3, HFS ed HFS+) come supporto per *Forensic Toolkit*; DIM-AM (*Digital Investigation Manager - Acquisition Module*), *freeware* sviluppato da *Dflabs* come supporto al *tool* DIM (*Digital Investigation Manager*); *Encase, tool* commerciale prodotto da *Guidance Software*; *Drive Snapshot*, sviluppato da Tom Ehlert; *Safeback, tool* commerciale

l'acquisizione; ma il minimo comun denominatore dell'attività di un tecnico che ha come obiettivo la preservazione della fonte di prova originale consta necessariamente dei seguenti addendi: il supporto di destinazione su cui si effettua la copia dei dati deve essere "vergine"[146]; il supporto sorgente non deve essere alterato durante la fase di acquisizione dei dati (qualora dovesse esserlo, deve essere possibile darne completa documentazione attraverso la c.d. catena di custodia).

Il problema consiste nel fatto che, nella maggiore parte dei casi, collegando un qualsiasi supporto di memorizzazione ad un dispositivo (operazione necessaria se si vuole "copiare" delle informazioni di natura digitale), si producono delle modifiche ai dati in esso contenuti[147]. Al fine di garantire l'integrità e la genuinità della prova digitale durante la procedura di acquisizione forense dei dati, è quindi necessario prevedere un "blocco" dell'accesso in scrittura sul supporto contenente i dati da copiare[148]. Solo così si garantisce la

---

sviluppato da NTI. Un *tool* molto utile, sempre in ambiente Windows, è *Mount Image Pro*, sviluppato da *Get Data*, che consente di montare in modalità "sola lettura" immagini in formato *dd*, *Encase* e *SMART*.

[146] «Perché tutto possa svolgersi nel modo più genuino possibile […] occorrerà a priori eseguire un'accurata inizializzazione dei supporti sui quali verrà raccolta l'evidenza digitale, adoperando procedure di *wiping* (distruzione sicura dei dati mediante diversi cicli di cancellazione) idonee ad assicurare che il supporto sul quale si effettuerà la copia non abbia nessun residuo di dati precedenti». Così, G. ZICCARDI, *Manuale breve di informatica giuridica*, Milano, 2008, p. 205. Questo significa procedere alla c.d. cancellazione sicura dei dati, anche precedentemente contenuti nel supporto. Gli utenti di sistemi operativi Microsoft Windows possono far riferimento alle pagine informative pubblicate dal produttore (http://www.microsoft.com/italy/pmi/sicurezza/privacy/), che illustrano nel dettaglio le modalità per affrontare il problema della cancellazione di interi volumi di dati. Gli utenti del sistema operativo Apple MacOS X, che incorpora una funzione di "svuotamento del cestino in modalità sicura", potranno trovare dettagliate informazioni sul sito del produttore www.apple.it oppure ricorrere a utility di tipo "open source" come *Permanent Eraser*, che consente di effettuare cancellazioni sicure con un algoritmo avanzato. Diversi applicativi software di tipo open source o comunque con licenze d'uso non commerciali sono poi disponibili per i sistemi Unix e Linux: tra questi, uno dei più noti ed efficaci è DBAN (www.dban.org).

[147] Queste modifiche possono riguardare, ad esempio, la data di ultimo accesso o di ultima modifica di un file (informazioni contenute nel c.d. file di *log*).

[148] Il c.d. *write blocking* può essere garantito sia a livello *software*, sia a livello *hardware*. Il blocco in scrittura a livello software si può ottenere agendo sull'operazione di *mounting* dell'hard disk da parte del sistema operativo. In generale quando un hard disk viene collegato ad un elaboratore, il sistema operativo lo mette a disposizione dell'utente per effettuare operazioni di lettura e scrittura. A seconda del sistema operativo utilizzato sulla macchina forense di acquisizione, si possono adottare opportuni accorgimenti per impedire il flusso bidirezionale della comunicazione e consentire un accesso in modalità di sola lettura. In ambiente Microsoft Windows (da Windows XP SP2 in avanti), è possibile agire a livello di registro di sistema per proteggere da scrittura i dispositivi USB. Una volta attivato questo blocco è possibile collegare l'hard disk da acquisire alla macchina forense, utilizzando un'adeguata interfaccia di conversione (USB/IDE, USB/SCSI, USB/S-ATA, ecc.). Alcuni utili *tool* gratuiti per il blocco in scrittura delle porte USB in ambiente Windows sono: *Bytescout USB Locker; Document Solutions USB Write Blocker*. In ambiente Linux i volumi possono essere montati direttamente in modalità *read only*. Le distribuzioni di acquisizione forense adottano questa tecnica. La scelta di un *write blocking software* è indubbiamente economica, perché non richiede l'acquisto di particolari dispositivi. Ovviamente il *digital forenser* deve testare costantemente la validità di questa metodologia con la nascita e lo sviluppo dei nuovi standard di connessione. Un write blocker hardware è invece un dispositivo fisico che viene interposto tra l'hard disk e la macchina di acquisizione forense (per questo motivo è anche detto *forensic bridge*). Questi dispositivi, oltre ad essere flessibili, facilmente trasportabili e semplici da utilizzare, sono anche più

"preservazione" della fonte di prova, consentendo alla controparte di "trattare" la stessa alle medesime condizioni. Una volta terminata l'acquisizione, è necessario garantire, provandolo, l'aderenza assoluta della copia rispetto all'originale. Tale scopo viene raggiunto attraverso un vero e proprio "sigillo digitale", che prende il nome di funzione di *hash*[149].

Ovviamente, e qui veniamo al secondo punto fondamentale per il processualista, tutta l'attività tecnica di acquisizione posta in essere in sede di accertamento urgente deve essere controllabile a posteriori. Dal punto di vista tecnico, ciò si traduce nella necessità di utilizzare software *open source*, i quali offrono la possibilità di consultare il codice sorgente, ossia il testo intelligibile del programma. Solo avendo accesso al contenuto intelligibile del programma è possibile -per un altro tecnico, in un altro momento- ripercorrere le tappe dell'operazione acquisitiva eseguita d'urgenza onde verificarne la correttezza metodologica[150]. Si è sostenuto, in particolare, che utilizzare software commerciali, o meglio ancora a "codice chiuso", non permetta l'effettiva valutazione alle parti delle specifiche del sistema utilizzato e, in particolare, del suo corretto funzionamento in termini di una giusta acquisizione dal momento che «non essendo possibile analizzare i codici-sorgente di questi programmi, la validità dei *report* da loro generati è fondata su un vero e proprio atto di fede»[151]. L'utilizzo di programmi accessibili e trasparenti si impone, quantomeno, nella fase di acquisizione urgente a causa della fisiologica mancanza di contraddittorio *ex ante* con la controparte[152].

---

comprensibili per interlocutori non tecnici (es. un giudice). Esistono anche modelli che possono essere installati in maniera permanente in un *bay* della *workstation* di acquisizione. I *write blocker* solitamente integrano diverse tipologie di interfaccia (IDE, SATA, SCSI, USB, Firewire ecc.) e vengono collegati alla macchina di acquisizione tramite connessione USB o *Firewire*. Necessitano di una fonte di alimentazione e vengono forniti con cavi di collegamento e conversione. I principali produttori di *write blocker* hardware sono: *Tableau; WiebeTech; Intelligent Computer Solutions; Voom Technologies; MyKey Technology; Digital Intelligence; Logicube; DIBS USA; Fernico*. Ovviamente esistono anche strumenti di *write blocking* per altri tipi di risorse, come i *card reader* forensi, che consentono un accesso in sola lettura durante il trattamento di schede di memoria (SD, SDC, XD, MMC, CF, ecc.). Alcuni produttori offrono, inoltre, dei kit di *write blocking* per rendere il *digital forenser* in grado di operare con il maggior numero possibile di interfacce e dispositivi differenti. Includono solitamente cavi, adattatori, strumenti di foto/video ripresa e buste isolanti per il trasporto degli hard disk.

[149] Cfr., *infra*, in questo capitolo.

[150] La controllabilità delle operazioni dipende dalla natura "proprietaria" o "aperta" del *software* utilizzato dall'esperto. Cfr. G. ZICCARDI, *Manuale breve*, cit., pp. 51 e ss.

[151] A. Monti, *Attendibilità dei sistemi di computer forensic*, http://www.ictlex.net/?p=287, 30 novembre 2015.

[152] «I software open-source rappresentano un ottimo strumento a basso costo, ed in ambito forense forniscono una grande opportunità perché permettono di trattare il reperto informatico con trasparenza operativa e garanzia, ed offrendo la possibilità di consultare il codice sorgente e conseguentemente di documentare i metodi e le tecniche utilizzate nella acquisizione dei reperti digitali. L'open-source, per le case produttrici di software commerciali per uso forense rappresenta anche un forte stimolo a migliorarsi per "competere" con questi tool che sono tendenzialmente gratuiti. Tuttavia non è sempre possibile utilizzare programmi open-source per tutte le problematiche. L'ideale sarebbe adoperare un sistema ibrido e servirsi di applicativi proprietari, come Encase o FTK, e software open source come Helix, ma non solo, in tutti quei casi dove si rende necessario documentare la

Ciò chiarito dal punto vista squisitamente tecnico, appare opportuno addentrarci ora nel versante più strettamente giuridico, certamente più familiare e più consono alla nostra formazione. Ebbene, secondo la giurisprudenza di legittimità l'attività di copia forense rappresenterebbe un'operazione sempre ripetibile in dibattimento, a patto che si agisca in modo tale da non alterare i dati originali[153]. Alla base di tale convincimento vi è la convinzione che le operazioni tecniche di natura digitale, se eseguite professionalmente ed a regola d'arte, sono insuscettibili di modificare l'oggetto dematerializzato[154].

All'estremità opposta, un orientamento di matrice dottrinale ravvisa sempre e comunque la natura non ripetibile delle attività tecniche di natura digitale a causa della sempre possibile alterazione dei *files* ad opera di *software forensics* mai completamente affidabili[155]. Sia che si parli di semplice lettura, sia che si proceda ad acquisire dati in forma digitale, in base a questa seconda tesi la modificabilità degli originali è *in re ipsa* e deriva dalla dematerialità dell'oggetto di indagine. La conseguenza di tale ragionamento è che il rispetto del diritto di difesa esige sempre che tali operazioni vengano eseguite con le forme dell'accertamento tecnico non ripetibile, *ex* art. 360 c.p.p.

Chi scrive è dell'opinione che entrambe le tesi sopra esposte pecchino di massimalismo, seppur di segno opposto. In base ad una terza e più moderata teoria, si ritiene inutile prendere posizione su tale questione da un punto di vista teorico e astratto: la valutazione deve necessariamente tener conto delle circostanze del caso concreto, ragionando in termini di

---

propria attività per l'assenza della parte interessata o per risolvere problematiche ben precise: a titolo di esempio, i "live cd" Linux sono l'unica alternativa per determinate acquisizioni. Spesso i forenser utilizzano software open-source per porsi al di sopra di ogni dubbio, utilizzandoli per l'acquisizione, mentre effettuano l'analisi dei dati con strumenti diversi per poi compararne i risultati. È bene quindi effettuare l'acquisizione dei dati, che rappresenta la fase più delicata ed esposta al rischio di alterazione del reperto, con software open-source, mentre le analisi dei reperti con comprovati software commerciali come Encase». Così, D. E. CACCAVELLA, *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, http://www.marcomattiucci.it/l482008.php, 30 novembre 2015

[153] «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». Cfr. Cass., sez. I, 5 marzo 2009, n. 14511, in *C.E.D. Cass.*, 243150; cfr., Cass., sez. I, 9 marzo 2011, in *Cass. pen.*, 2012, p. 440, con nota di M. DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*.

[154] Cfr., ancora più chiaramente su questo punto, Cass. pen., sez. I, 26 febbraio 2009, n. 11863, in *CED Cass.*¸ 2009, n. 243922, secondo cui «l'estrazione dei dati contenuti in un supporto informatico, se eseguita da personale esperto in grado di evitare la perdita dei medesimi dati, costituisce un accertamento tecnico ripetibile».

[155] Cfr. L. LUPARIA - G. ZICCARDI, *Investigazione penale e tecnologica informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali,* cit., pp. 154 e ss.; E. M. MANCUSO, *L'acquisizione di contenuti e-mail*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, pp. 53 e ss.

urgenza piuttosto che di irripetibilità[156]. Probabilmente, quest'ultima opzione ermeneutica coglie nel segno, soprattutto perché consente di tener conto della complessità del fenomeno in esame. Sul piano operativo bisogna acquisire un atteggiamento pragmatico: è velleitario pensare di attuare garanzie assolute in ogni versante e in ogni profilo dell'accertamento dei reati. Il problema di fornire le dovute garanzie durante l'acquisizione delle fonti di prova è una peculiarità caratterizzante tutta l'attività di polizia giudiziaria non ripetibile. Tuttavia, ci sono attività da svolgere nell'immediatezza del fatto che non sempre consentono la tempestiva instaurazione del contraddittorio e non sopportano differimento, pena il pregiudizio irrimediabile dell'ulteriore corso delle indagini. I due termini estremi della questione sono da un lato la non rinviabilità di alcune azioni accertative, dall'altro la paralisi del controllo difensivo in assenza di adeguato contraddittorio. Tra i due estremi, l'area di compromesso deve tener conto che non ogni modificazione è concretamente rilevante e non ogni azione accertativa è insuscettibile del breve differimento necessario ad assicurare la presenza del difensore. Ove il compromesso sia impraticabile, alle garanzie della difesa e al processo di formazione del convincimento del giudice può soccorrere il controllo esercitatile *ex* post mediante un'adeguata documentazione dell'attività accertativa, tale da poter verificare l'effettiva incidenza di essa sui risultati conseguiti.

Punto di partenza della riflessione è che le regole tecniche debbono piegarsi a quelle processuali e non viceversa. Il codice di procedura penale del 1988 impone, come regola, che le prove si formino in contraddittorio in modo tale che le parti possano contribuire fattivamente alla loro formazione. Ovviamente, esistono delle eccezioni alla regola, ma, proprio perché eccezionali, tali ipotesi devono essere interpretate in maniera restrittiva. Ebbene, proprio la necessità di garantire il contraddittorio tecnico sull'evidenza digitale impone all'interprete di fare chiarezza.

In tema di *digital evidence*, la scienza mette in guardia il processualista: l'acquisizione potrebbe inevitabilmente provocare modifiche irreversibili sui dati a prescindere dalla volontà e dalla competenza degli operatori. Quindi, il rispetto del principio del contraddittorio impone che la regola sia l'utilizzo, da parte degli inquirenti, dell'art. 360 c.p.p. Eccezionalmente, è consentito il ricorso all'art. 354 c.p.p. in ipotesi di urgenza (leggasi, indifferibilità) dell'accertamento. Tuttavia, anche quando si procede unilateralmente tramite accertamento urgente è necessario garantire, quantomeno, il contraddittorio postumo sull'elemento di prova

[156] Cfr. A. CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, Padova, 2014, pp. 68 e ss.

digitale acquisito. Ciò impone, innanzitutto, che l'estrapolazione dei dati avvenga con una metodologia tale da garantire le minori modifiche possibili e la conservazione delle informazioni acquisite.

Chi scrive è ben cosciente della estrema "delicatezza" dell'operazione tecnica di acquisizione di dati digitali da una fonte di prova informatica: qualsiasi errore in tale fase si ripercuote inevitabilmente sul valore investigativo e processuale dell'intera evidenza digitale potenzialmente disponibile. Proprio per tale motivo, l'opportunità di procedere *on site* alla immediata duplicazione dovrebbe dipendere dalle circostanze concrete in cui si rende necessario effettuare tale "trattamento". In altre parole, avendo come obiettivo la intangibilità dei dati da acquisire, a ciascuna situazione operativa concreta deve corrispondere un diverso protocollo operativo, ossia una diversa *best practice* da implementare al fine di raggiungere gli obiettivi di affidabilità della fonte e di genuinità dell'elemento di prova indicati dal codice. D'altronde, il codice individua gli obiettivi, ma i modi per raggiungerli sono diversi e variano al variare del contesto operativo di riferimento[157].

In particolare: 1) se il sistema non è in funzione e l'acquisizione dei dati non riveste carattere d'urgenza, potrà essere ragionevolmente posticipata in laboratorio la materiale apprensione dei *files* dal supporto che li contiene, ovviamente previa instaurazione del contraddittorio con la difesa, *ex* art. 360 c.p.p.; nella preliminare e propedeutica fase di primo intervento, invece, ci si dovrebbe limitare al sequestro materiale del supporto, opportunamente repertato[158]. Ed infatti, una regola fondamentale, che può sembrare banale ma che rappresenta la più importante di tutte le complesse procedure legate alle attività di

[157] «Diverso, infatti, è il trattamento tecnico da riservare a dispositivi rinvenuti in modalità off o on. Si pensi al caso di ritrovamento sulla scena del crimine di due computer, di cui solo uno acceso. Nel caso di computer spento gli inquirenti, qualora lo ritengano necessario, potranno esaminarne preliminarmente il contenuto e procedere eventualmente a sequestro dell'intero hard-disk o di alcune parti attraverso il ricorso alle procedure previste: ciò che preme rilevare è che in tale ipotesi, il rischio di alterabilità dei dati presenti è più basso rispetto al caso opposto, sempreché in via preliminare siano adottate le cautele previste dalle best practices. La questione risulta invece più complessa nel caso in cui il dispositivo sia acceso e collegato alla rete: in questa ipotesi la prescrizione prevista dall'art. 247, comma 1-*bis* c.p.p. acquista un peso e una rilevanza ancor più imprescindibile stante l'alto tasso di vulnerabilità del sistema dato dalla sua dinamicità. "Frugare" all'interno di un sistema attivo è attività molto rischiosa che interessa sia la genuinità dei dati rinvenuti al momento dell'atto, sia il tema delle garanzie difensive, rappresentandosi come attività sostanzialmente non ripetibile. Ciò comporta il richiamo all'art. 360 in tema di accertamenti urgenti i quali, tuttavia, non sempre possono essere praticati, vuoi per la natura stessa dell'istituto che è e resta tipico atto d'indagine a sorpresa, vuoi per impossibilità legate al caso concreto (se si proceda contro ignoti, se vi sia una quantità enorme di dati da acquisire, se il target sia rappresentato per esempio da Service Provider, istituti bancari, gestori di telefonia e in generale in tutti i casi in cui possano sorgere problemi sulla qualità del servizio reso dal soggetto interessato a perquisizione)». Così, C. MAIOLI - E. SANGUEDOLCE, *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, www.altalex.com, 30 novembre 2015.

[158] Tutti i dispositivi spenti al momento del sopralluogo dovrebbero essere riposti in buste antistatiche, per il loro successivo trasporto e analisi in laboratorio.

digital forensics, è quella di evitare nella maniera più assoluta di accedere al dispositivo, ovvero di interagire in qualsiasi modo con le evidenze rilevate sulla scena. La mera accensione di un computer, di un cellulare o di un qualunque dispositivo che abbia capacità computazionali provoca un'interazione tra dati, memorie e sistema operativo che, in termini di gestione forense dell'evidenza, deve sempre essere considerata come un'alterazione di tali dati e dunque del reperto stesso; 2) se il sistema non è in funzione, ma è comunque necessario dare immediato corso all'acquisizione dei dati per esigenze investigative, si procederà all'avvio della macchina ed all'acquisizione dei dati digitali *on site* attraverso una procedura in grado di evitare la alterazione dello *status quo*[159]; 3) se il sistema è in funzione, ma è possibile sequestrarlo per analizzarlo in seguito, si procederà al suo spegnimento mediante una procedura che garantisca l'integrità di tutti i dati presenti[160]. Anche il semplice spegnimento della macchina deve seguire un preciso protocollo, che dipende, in genere, dal sistema operativo utilizzato dal dispositivo oggetto di interesse investigativo. Con alcuni sistemi operativi, il metodo preferibile è quello di schiacciare il pulsante di spegnimento della macchina; con altri sistemi, invece, questo comporterebbe la irrimediabile perdita di dati e di informazioni, sicché è di gran lunga preferibile "staccare la spina"[161]; 4) se il sistema è in funzione ed è altresì necessario, per esigenze investigative o tecniche, procedere all'acquisizione dei dati *on site*, dovrà essere utilizzata, ancora una volta, una procedura che,

---

[159] In questo caso, l'avvio della macchina non deve avvenire secondo la procedura ordinaria. Infatti, il solo avvio del sistema operativo e degli altri programmi specificati nel *file system* e programmati per essere eseguiti automaticamente all'accensione, potrebbe alterare alcuni dati del dispositivo (quali, ad esempio, i dati contenuti nei vari registri cronologici, i dati contenuti nella memoria virtuale, ecc.). Per evitare alterazioni, dopo aver disconnesso i supporti da analizzare, si deve procedere all'avvio del sistema tramite accesso al BIOS. Dalle impostazioni di quest'ultimo, è possibile far sì che l'avvio del sistema avvenga tramite il software contenuto in un dispositivo esterno. Solo dopo aver eseguito tale operazione di potranno ricollegare i supporti da analizzare. Quindi, si potrà avviare la macchina, che, a questo punto, prenderà le informazioni utili all' "avvio controllato" dal dispositivo esterno appositamente indicato in fase di impostazione del BIOS. In tale dispositivo, ovviamente sarò contenuto un programma che avvierà la copia *bit stream* di quanto contenuto nei supporti.

[160] Per un approfondimento, cfr. G. ZICCARDI, *Manuale breve*, cit., pp. 208 e 209.

[161] In alcuni casi, quando viene rinvenuto un elaboratore acceso viene consigliato di togliere l'alimentazione agendo sulla presa di corrente, invece che effettuare le comuni procedure di spegnimento del sistema. Tale risulta essere, infatti, la soluzione meno distruttiva in termini di conservazione della prova informatica. E' indubbio come una operazione così drastica possa rilevare dubbi sulla effettiva correttezza metodologica, bisogna però considerare, in estrema ratio, che la priorità ultima non è preservare il sistema nel suo complesso ma l'evidenza informatica nello specifico. Togliere la spina lato elaboratore e non lato presa a muro produce un immediato spegnimento della macchina con conseguente congelamento di ogni eventuale attività, preservando eventuali informazioni presenti in cache non volatili o nei file temporanei. Senza contare il fatto che esistono specifici applicativi che installati rimangono silenti ed invisibili all'operatore e possono essere impostati in modo da distruggere determinate porzioni di disco nel momento in cui si effettuano le normali procedure di spegnimento.

rispettosa della necessità di garantire l'integrità dei dati, rappresenti un giusto compromesso tra l'esigenza di continuità del sistema e quella di rapidità dell'esecuzione.

Nelle ipotesi sub 1) e sub 3), l'acquisizione è giuridicamente inquadrabile come attività di natura tecnica connotata da irripetibilità ma priva del requisito dell'urgenza[162]. Di conseguenza, la copia forense dovrebbe essere fatta in laboratorio, nel rispetto del contraddittorio, seppur debole, di cui all'art. 360 c.p.p. In sede di sopralluogo, invece, bisognerebbe limitarsi al sequestro materiale del supporto.

La medesima attività, nelle ipotesi sub 2) e sub 4), invece, è caratterizzata sia dalla non ripetibilità[163], sia dall'urgenza. Ergo, l'acquisizione deve avvenire necessariamente *on site*, nel rispetto dei protocolli indicati dalle *best practices*. In tale contesto si pone il problema della c.d. *live data forensics*: l'intervento dell'operatore di polizia giudiziaria dovrà essere ben documentato[164] e ridotto al minimo necessario alle indagini. In questo caso, le procedure di acquisizione dovranno orientarsi alla minor invasività possibile. Nella pratica si dovranno adottare metodologie tecniche, differenziate in base alla tipologia di dispositivo da acquisire, che tenderanno ad un approccio alla prova in modalità *read-only*, ovvero alla "lettura" del contenuto del dispositivo senza introdurre alcuna modifica su di esso[165].

---

[162] Si tratta di rilievi la cui irripetibilità deriva dal fatto che il loro compimento, in qualche modo, altera, disperde o comunque modifica l'elemento di prova: è vero che una volta compiuti tali rilievi non potranno più essere utilmente ripetuti una seconda volta, ma è altrettanto vero che la scelta della prima volta in cui compierli è rimessa alla discrezionalità dell'operatore e non all'urgenza della situazione operativa concreta. In dottrina, cfr A. CHELO, *Rilievi irripetibili di p.g. o accertamenti tecnici irripetibili?*, in *Dir. pen. proc.*, 2014, 2, p. 209, il quale, molto acutamente, li definisce «rilievi ora e mai più».

[163] Si tratta di rilievi la cui irripetibilità discende dall'impossibilità di compiere il rilievo, alle medesime condizioni, in un secondo momento: in questo caso, al fatto che tali rilievi possono essere utilmente compiuti solo una volta, perché il loro compimento modifica lo stato delle cose, si aggiunge il fatto che la scelta circa il momento in cui compierli non è rimessa alla parte, ma deriva dall'urgenza del caso concreto. In dottrina, A. CHELO, *Rilievi irripetibili di p.g. o accertamenti tecnici irripetibili?*, cit., p. 209, li chiama «rilievi ora o mai più». V, *amplius*, A. CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, cit., pp. 68 e ss.

[164] «Ove si tratti di computer dell'indagato, la presenza di quest'ultimo (e quella del difensore) sul luogo dell'accertamento rende maggiore – anche dal punto di vista giuridico – il grado di resistenza di tali accertamenti in dibattimento».Così, F. CAJANI, *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, su http://www.marcomattiucci.it/l482008.php, 30 novembre 2015

[165] Non solo a livello informatico –penso all'*hash* apposto ai dati estratti– ma anche a livello di tradizionale, mediante l'utilizzo di riprese audio-visive. «Dal punto di vista squisitamente metodologico, andrebbe massimizzata la documentazione di queste attività così come, in generale, la trasparenza delle procedure. E di conseguenza sarebbe auspicabile utilizzare tecnologie open source, o quantomeno strumenti che forniscano adeguate garanzie. Dovrebbero essere garantiti non solo gli strumenti ma anche le metodologie di acquisizione dei reperti informatici, e fare in modo che l'acquisizione sia completa e che non inquini il dato […] Il problema è che tutto ciò che si può fare non dà garanzie totali, perché la controparte non ha modo di ripetere le attività di acquisizione e di apprezzare cosa è stato alterato e cosa no: per questo ribadisco che bisogna massimizzare la documentazione e minimizzare l'alterazione del reperto. Le acquisizioni on site forniscono dati esposti al pregiudizio di non essere attendibili, dai quali però si può partire per trovare elementi di attendibilità: per questo la live data forensics è una delle problematiche emergenti dell'informatica forense. Ci troveremo sempre di più

Evidentemente, spetta agli inquirenti valutare se nel caso concreto occorra disporre un sequestro 'materiale' dei supporti o effettuare un'acquisizione 'dematerializzata' dei dati, mediante *bit stream image*[166]. Con la seguente precisazione: «l'accertamento, come atto di acquisizione unilaterale, è ammesso soltanto (e a condizione) che sia possibile assicurare l'oggetto non soltanto in modo inalterato, ma anche in modo che le parti possano controllare successivamente l'affidabilità della fonte e la genuinità dell'elemento di prova»[167]. In ipotesi di *live data forensics*, questo fondamentale principio, posto a tutela di quel nucleo insopprimibile del contraddittorio inteso come metodo di accertamento, potrà ritenersi rispettato quando, quantomeno, le procedure e gli strumenti utilizzati risultino il meno invasivi possibile e quando le inevitabili -perché fisiologiche- alterazioni prodotte siano note e documentate[168]. In questo caso, la controllabilità *ex post* del metodo assurge a garanzia

---

in contesti in cui non ci saranno "semplicemente" dei dischi rigidi da acquisire, ma si verificheranno situazioni in cui i dati saranno volatili, siano essi contenuti nella RAM quanto nei pacchetti veicolati dalla Rete. Questo tipo di analisi forense sottintende il dover sacrificare qualcosa, come il medico legale che per poter determinare le cause della morte di un soggetto, deve poter incidere il cadavere per svolgere l'esame autoptico. Tuttavia nella *live forensics* l'invasività di alcune procedure di acquisizione può essere minimizzata, ad esempio facendo in modo che i programmi utilizzati per il *dump* della RAM vengano montati in settori di memoria non allocati. Nondimeno, la controparte potrebbe lamentare delle limitazioni alla propria attività difensiva, asserendo che l'impiego dello strumento utilizzato per il *dump* della RAM ha rimosso proprio quei settori della memoria che contenevano le fonti di prova utili a determinare l'innocenza del proprio assistito. La questione è dunque molto delicata in questi casi, a differenza della *network forensics* dove l'acquisizione contestuale dei dati non turba il sistema, dato che ci si "mette in ascolto" registrando il traffico dati». Così, D. E. CACCAVELLA, *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, http://www.marcomattiucci.it/l482008.php, 30 novembre 2015.

[166] «L'ispezione informatica (volta alla ricerca di dati presenti su computer) da effettuarsi on site si impone, di regola: laddove il computer da acquisire non sia ben identificabile; quando interessino solamente dati intesi come informazioni utili per l'immediato proseguo delle indagini, senza che sia necessaria l'apprensione fisica dell'intera macchina che li contiene; quando, anche laddove ci interessi l'apprensione fisica dell'intera macchina tramite sequestro, essa sia di difficile realizzazione: penso all'ipotesi di scuola di ricercare dati - utili agli investigatori – sui grandi server di società. […]. Se posso correttamente (ovvero in fatto, perché ritengo di averlo identificato, ed in diritto, perché ne sussiste la necessità probatoria) porre sotto sequestro un computer ed acquisirne successivamente i dati presenti nel laboratorio della PG, preferisco un giorno in più e una contestazione tecnica in meno». Così, F. CAJANI, *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, http://www.marcomattiucci.it/l482008.php, 30 novembre 2015. Cfr., inoltre, F. NOVARIO, *Criminalità informatica e sequestro probatorio: le modifiche introdotte dalla l. 18 marzo 2008, n. 48 al codice di procedura penale*, cit., p. 1070.

[167] «Questo costituisce il nucleo insopprimibile del contraddittorio come metodo di accertamento. Al tempo stesso, il contraddittorio esercitabile *ex post* esprime il principio del bilanciamento degli interessi contrapposti, come è stato elaborato dalla giurisprudenza costituzionale in altre occasioni. L'esigenza di ammettere la prova quando vi è «accertata impossibilità di natura oggettiva» (art. 111, comma 5 Cost.) non esclude, ed anzi impone, che sia tutelato quanto meno il contraddittorio "sulla prova" come nucleo insopprimibile della garanzia costituzionale. Naturalmente, il contraddittorio sulla prova è possibile soltanto alle predette condizioni; non è possibile quando un'acquisizione unilaterale ha modificato l'elemento di prova, o ha impedito di controllare l'affidabilità della fonte e la genuinità dell'elemento. In tal caso, la garanzia del contraddittorio sulla prova già assunta, ma in modo non corretto, risulta preclusa in radice». Così, P. TONINI, *Il documento informatico: problematiche civilistiche e penalistiche a confronto*, cit., p. 435.

[168] «Intervenire su un sistema live significa […] inevitabilmente perturbarlo, e svolgere quindi un accertamento che non potrà in nessun caso considerarsi ripetibile. Le procedure e gli strumenti devono comunque essere il

irrinunciabile: non importa provare ad ogni costo, ciò che conta è avere una prova controllabile, poiché il fine non giustifica i mezzi (la procedura), ma sono i mezzi a legittimare il fine[169].

2.3 Conservazione dell'evidenza digitale

Il terzo *step* consiste nella adozione di cautele idonee a garantire la "conservazione" dei dati digitali, tanto degli originali, quanto delle copie. In particolare, "conservare" un elemento di natura digitale significa garantirne l'integrità[170] (assenza di fattori esterni di alterazione) e documentarne la vita *post* acquisizione (attraverso la c.d. catena di custodia).

Tecnicamente, l'obiettivo della conservazione in ambito digitale presuppone l'adozione di cautele diverse a seconda che si parli di preservazione fisica o logica. Nel caso in cui le circostanze del caso concreto suggeriscano di sequestrare fisicamente il dispositivo hardware, il cui contenuto informativo sarà oggetto di una successiva analisi svolta in *post mortem*, l'operatore dovrà procedere all'imballaggio del dispositivo apponendo più etichette di sicurezza la cui rimozione, anche parziale, evidenzierà una violazione dei sigilli. Durante il periodo di tempo intercorrente tra il momento del materiale sequestro e quello dell'accertamento tecnico sul reperto, è necessario evitare pericoli di inquinamento, che, con riferimento a materiale informatico, sono per lo più rappresentati da esposizione a temperature estreme, umidità, raggi UV, vibrazioni durante l'uso od il trasporto, cadute (anche accidentali), campi elettromagnetici, ecc.[171]. Occorre quindi mettere in atto procedure che consentano una corretta conservazione della prova digitale, utilizzando ad esempio appositi contenitori o buste antistatiche e depositando i corpi di reato digitali presso archivi che

---

meno invasivi possibile: limitare l'inquinamento del reperto consentirà di acquisire più informazioni genuine. Le inevitabili alterazioni prodotte, infine, devono essere note e documentabili. In questo contesto non va comunque dimenticato uno dei principi fondamentali delle indagini digitali: quando è possibile scegliere tra acquisizione e analisi, prima si acquisisce e poi si analizza, non il contrario. Anche perché, solitamente, le procedure di acquisizione impattano sul sistema in misura minore rispetto ad operazioni di analisi». Così. D. GABRINI, *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, http://www.marcomattiucci.it/l482008.php, 30 novembre 2015.

[169] In questo si sintetizza la differenza tra lo storico ed il giudice. Cfr. P. TONINI, *Manuale di procedura penale*, cit., pp. 259 e ss.

[170] L'integrità dipende dalle cautele adottate in concreto per evitare il danneggiamento, anche accidentale, dei dati. I problemi principali in un laboratorio forense sono legati a: elevata quantità di dati; necessità di trasferimento dei dati; necessità di conservazione dei dati integri per lungo tempo; necessità di garantire un accesso riservato ai dati. Per soddisfare queste necessità è necessario implementare una accurata policy di Data Management.

[171] U.S. Department of Justice, *Electronic crime scene investigation: a guide to First Responder*, https://www.ncjrs.gov/pdffiles1/nij/219941.pdf, 30 novembre 2015.

garantiscano condizioni di temperatura ed umidità costanti, privi di luce naturale ed adeguatamente schermati dal punto di vista elettromagnetico[172]. Tali archivi dovrebbero altresì prevedere sistemi di protezione fisici ad accesso condizionato, con registrazione di ogni singola apertura. Il personale che interagisce con i reperti dovrà indossare appositi dispositivi antistatici, utilizzando strumentazione idonea nel momento in cui il reperto sarà aperto per essere esaminato.

Quando è possibile acquisire i dati *on site* in sicurezza, la conservazione deve essere realizzata innanzitutto a livello software, con memorizzazione del clone all'interno di un c.d. *forensic container*[173] e validazione del suo contenuto informativo attraverso un doppio codice *hash*[174]. Nel linguaggio matematico ed informatico, la funzione *hash* è una funzione univoca, unidirezionale e non invertibile, che consente di codificare una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. In particolare, l'algoritmo di *hash*, partendo da un documento di qualsiasi tipo e grandezza, è in grado di generare una stringa univoca di dimensioni fisse denominata *digest* o impronta digitale. Applicando tale algoritmo al contenuto di un file o anche ad un intero dispositivo, si ottiene una sequenza alfanumerica di caratteri che rappresenterà l'impronta digitale dei dati memorizzati nel dispositivo. Il valore di *hash* del dato originario e del suo clone, calcolato in sede di repertazione, sarà dunque il sigillo digitale dell'evidenza e costituirà una certificazione inoppugnabile che il contenuto del supporto originale risulti esattamente uguale alla copia; ciò in quanto una minima modifica degli elementi acquisiti genererà un *digest* differente rispetto a quello prodotto in sede di acquisizione del contenuto del dispositivo originale, inficiandone il valore processuale[175].

---

[172] E' noto come le cariche elettrostatiche o forti campi elettromagnetici possano interagire con i dati contenuti all'interno di tutti quei dispositivi di memorizzazione di tipo read-write, come ad esempio Hard disk, floppy disk, pen drive, memorie allo stato solido, memorie ad accesso casuale (RAM, ROM) etc. I soli dispositivi apparentemente non influenzabili da campi elettromagnetici sono i dispositivi ottici quali CD-ROM o DVD-ROM, etc., che comunque possono essere soggetti a degrado in particolare se vengono a contatto con sostanze solventi o composti solforosi.

[173] Un *forensic container* è caratterizzato dai seguenti elementi: controlli interni sulla consistenza dei dati (integrità, indicizzazione, ecc.); informazioni sul caso investigativo (numero del caso, descrizione del supporto, nominativo dell'operatore, ecc.; sistemi di compressione; sistemi di cifratura.

[174] L'integrità dei dati oggetto di acquisizione può essere garantita e verificata attraverso l'applicazione di un algoritmo di *hash*, che consente di "firmare" in maniera univoca un determinato agglomerato di dati. Cfr., per un approfondimento, G. ZICCARDI, *Manuale breve*, cit., pp. 206 e 207.

[175] D'altronde, una verifica bit-a-bit richiede tempi di elaborazione molto elevati. Per questo motivo si utilizzano funzioni di *hash*. Una funzione di *hash* è una funzione one-way che, dato un input di lunghezza arbitraria, fornisce un output (*hash*) di lunghezza fissa. Dall'*hash* non è possibile risalire al dato originale ed una minima variazione nel dato originale si traduce in una grande variazione del risultato. Queste proprietà rendono le funzioni di *hash* lo strumento ideale per la verifica di una copia forense: si calcola l'*hash* dell'originale e quello della copia; se coincidono, allora anche originale e copia coincidono. Le principali funzioni di *hash* utilizzate sono: MD5 (*Message Digest Algorithm*); SHA-0, SHA-1, SHA-2 (*Secure Hash Algorithm*). La maggior parte dei

Garantire una corretta catena di custodia significa documentare tutto ciò che è stato fatto con la prova originale e con le copie forensi realizzate, a partire dall'acquisizione fino ad arrivare al giorno del processo. Il primo anello della catena di custodia è costituito dal c.d. *first responder*: il primo e forse anche l'unico soggetto a vedere la scena del crimine nel suo stato originale.

Il primo atto di una corretta catena di custodia nasce dal sopralluogo e dal relativo sequestro: all'esito di tali attività, infatti, il codice di rito contempla l'obbligo di verbalizzazione. Tipiche informazioni che possono essere contenute inizialmente in questi verbali sono: numero del caso; reparto investigativo; investigatore assegnato al caso; natura e breve descrizione del caso; investigatore incaricato della duplicazione dei dati; data e ora di inizio custodia; luogo in cui il supporto è stato rinvenuto; produttore del supporto; modello del supporto; numero di serie del supporto. Ogni volta che i supporti oggetto di indagini vengono affidati ad un nuovo investigatore, ad un perito, ad un consulente tecnico di parte o all'ufficio dei corpi di reato del Tribunale, nella catena di custodia dovrà essere aggiunta un'informazione contenente i seguenti elementi: nome dell'incaricato all'analisi; data e ora di presa in carico del supporto; data e ora di restituzione del supporto.

Giuridicamente, conservazione e documentazione sono imposte dal principio del contraddittorio nella formazione della prova: l'evidenza digitale deve essere conservata in modo tale da essere preservata da qualsiasi possibile alterazione, per consentire alla controparte di esperire le relative indagini, perizie e valutazioni su un *quid* identico all'originale.

2.4 Analisi dei dati e presentazione dei risultati

Quarto *step:* una volta acquisiti i dati, il *digital forenser* deve occuparsi di analizzarli scientificamente alla ricerca di elementi processualmente rilevanti. Attraverso specifici *software* è possibile estrapolare dal contenuto dei *files* tutta una serie di informazioni che possono tornare utili ai fini delle strategie processuali delle parti[176]. Ovviamente, la quantità e

---

programmi di acquisizione, sia in ambiente Linux che in ambiente Windows, integrano al loro interno il calcolo ed il confronto degli *hash*. Un programma *opensource* e multipiattaforma utile per il calcolo dell'*hash* è MD5Deep.

[176] A seconda dei casi si dovranno analizzare: documenti (DOC, XLS, PDF, ecc.); immagini; posta elettronica; navigazione web; chat ed *instant messaging*; database; file di log; registri di sistema; *active Data Stream*; file cancellati; file nascosti; *slack space; bad blocks*; file cifrati; partizioni cifrate; partizioni nascoste; memorie

la qualità delle informazioni utili estrapolabili sono direttamente proporzionali alla complessità dello strumento software ed alla competenza del consulente tecnico che lo utilizza.

Giuridicamente, le norme di riferimento sono diverse a seconda della fase procedimentale in cui si rende necessaria l'analisi: «in sede di indagine preliminare sarà possibile, alternativamente, procedere ad accertamenti tecnici (artt. 359 e 360 c.p.p.) o ad incidente probatorio (artt. 392 e ss. c.p.p.); in sede dibattimentale, invece, sarà possibile utilizzare lo strumento della perizia (artt. 220 e ss. c.p.p.)»[177].

Alla luce di quanto abbiamo detto sinora, l'accertamento tecnico digitale preceduto da regolare duplicazione, in quanto idoneo ad essere ripetuto nuovamente in giudizio tramite perizia, non è mai qualificabile come atto irripetibile[178], come tale suscettibile di automatica acquisizione dibattimentale; di contro, l'accertamento tecnico digitale non preceduto da rituale clonazione forense è atto non ripetibile perché determina una modifica irreversibile della realtà da analizzare, di talché si rende necessario attivare il contraddittorio preventivo di cui all'art. 360 c.p.p.[179].

Tecnicamente, nell'analisi di un dispositivo digitale si dovrà procedere dal generale al particolare, al fine di poter ricavare in maniera puntuale ogni eventuale elemento utile. Si inizierà con una descrizione sommaria del sistema[180] sino ad arrivare al singolo applicativo o al file oggetto di ricerca[181]. Senza alcuna pretesa di esaustività, le principali attività che è possibile compiere su di un dispositivo digitale sono le seguenti: *text searching*, ossia ricerche di tipo testuale all'interno dei file o delle directory; *image searching*, che consiste nella ricerca delle immagini digitali presenti all'interno di un file nei diversi formati tecnicamente possibili; *data recovery*, *data discovery* e *data carving*, consistenti in procedimenti tecnici

---

volativi (RAM). La metodologia di analisi varia considerevolmente al variare del *file system* e del sistema operativo eventualmente installato sul supporto originale.

[177] Così, G. VACIAGO, *Profili processuali delle indagini informatiche*, in G. CASSANO – G. SCORZA – G. VACIAGO (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Padova, 2013, p. 651.

[178] Cfr. F. NOVARIO, *Le prove informatiche nel processo civile*, Torino, 2014, p. 130, secondo sui l'accertamento tecnico in sede informatico-forense rientra nell'ambito dell'art. 359 c.p.p. nella misura in cui non ha ad oggetto la creazione di una copia forense dei dati, quanto, piuttosto, l'analisi degli stessi una volta cristallizzati dalla polizia giudiziaria.

[179] Cfr. L. LUPARIA – G. ZICCARDI, *Investigazione penale e tecnologia informatica*, cit., p. 154, nonché E. M. MANCUSO, *L'acquisizione di contenuti e-mail*, in A. SCALFATI (a cura di), *Le indagini atipiche*, cit., pp. 53 e ss.

[180] Sistema operativo, programmi o applicativi presenti, date di installazione, di utilizzo, ultimo accesso e ultimo spegnimento del dispositivo, utenti presenti e relativi privilegi di accesso, etc. Occorrerà poi verificare la presenza di sistemi ad accesso condizionato o l'uso di password, l'eventuale stato di aggiornamento del sistema, nonché il livello di sicurezza presente (antivirus, *firewall* ecc.).

[181] Ma anche alle aree cancellate, non più utilizzate, non allocate, sino allo *slack space*, ecc.

finalizzati a recuperare dalla memoria del dispositivo dati cancellati o danneggiati, dati nascosti, cifrati o protetti in altro modo[182]; *metadata recovery*, ossia recupero delle informazioni di sistema poste a corredo della struttura del file system, dei file, delle cartelle o delle partizioni.

I risultati raggiunti attraverso l'elaborazione critica dei dati digitali vengono solitamente profusi in una relazione tecnica: «questo documento deve descrivere tutte le operazioni compiute per il raggiungimento del risultato dell'analisi del dato digitale; in tale sede, sarà necessario operare uno sforzo di sintesi e di semplificazione, tale da abbattere ogni potenziale *digital divide* tra inquirenti e giudicanti»[183].

3. I mezzi di ricerca della prova di natura digitale: ispezioni, perquisizioni, sequestri

3.1 Ispezione tradizionale e ispezione informatica

Una constatazione, in premessa, non appare superflua: nonostante i pochi articoli che il codice di rito gli dedica, l'istituto dell'ispezione ha sollevato e continua a sollevare notevoli problematiche, tutte collegate essenzialmente alla necessità di conciliare accertamento del fatto e rispetto del diritto di difesa, i quali rischiano la collisione in un atto, quello ispettivo appunto, che, una volta compiuto durante la fase delle indagini preliminari, difficilmente appare ripetibile nel corso del processo. Tali problematiche, anziché sopirsi nel corso del tempo, trovano nuovo e fertile terreno a seguito dell'introduzione, nel 2008, della c.d. "ispezione informatica", in cui, come vedremo, «il fondato motivo di ritenere che le tracce o gli altri effetti materiali del reato possano essere alterati» di cui all'art. 245 c.p.p., utile ai fini dell'omesso avviso al difensore, è *in re ipsa* a causa della ontologica volatilità del dato digitale.

Etimologicamente, il vocabolo "ispezione" deriva dal latino *inspiciens*, participio presente di *inspicere*, cioè "guardare in qualcosa"[184]. Nel linguaggio comune, quando si parla di ispezione ci si riferisce ad un esame, ad una osservazione attenta di una cosa, di un luogo o di

---

[182] Sul problema relativo al delicato rapporto esistente tra la crittografia e le garanzie dell'indagato, cfr. G. VACIAGO, *Profili processuali delle indagini informatiche*, cit., p.p. 654 e ss.
[183] G. VACIAGO, *Profili processuali delle indagini informatiche*, cit., p. 653.
[184] F. CORDERO, *Procedura penale*, 8^ ed., Milano, 2006, p. 828.

una persona. Processualmente, ispezione significa percezione visiva, rectius, sensoriale, di una cosa pertinente al reato per cui si procede. In particolare, l'ispezione è un mezzo tipico di ricerca della prova finalizzato ad «acquisire prove materiali, tracce o dichiarazioni dotate di attitudine probatoria»[185]. In altre parole, l'ispezione consente di acquisire elementi rilevanti e talvolta decisivi che, tuttavia, si trovano al di fuori del processo e vanno quindi ricercati[186]. L'esito di tale ricerca è una «prova precostituita al processo»[187]. Quanto all'essenza di siffatta operazione di ricerca, l'ispezione si caratterizza per la diretta osservazione di elementi utili alla ricostruzione dei fatti, attraverso la semplice «constatazione e rilevazione di dati obbiettivi pertinenti all'ipotesi di reato per cui si procede»[188]. Pertanto, essa si caratterizza per la sua «limitazione all'obiettivo esame e rilevamento di una situazione di fatto attuale, come essa cade sotto i sensi dell'organo procedente»[189]. In altre e più semplici parole, nell'ispezione la ricerca si traduce in osservazione e constatazione, senza alcuna interferenza fisica dell'operatore sullo stato delle cose. L'unico strumento che si frappone tra l'inquirente e la *scena criminis* è lo sguardo di chi osserva: «*inspectio* evoca occhi esploranti»[190].

Tale caratteristica serve a distinguere nettamente l'ispezione da altri mezzi di prova e di ricerca della prova affini: rispetto alla perquisizione, essa si differenzia per il fatto che, a ben guardare, manca una vera e propria attività di ricerca, limitandosi l'operato dell'inquirente ad una semplice osservazione della realtà opportunamente verbalizzata; rispetto all'esperimento giudiziale, il *discrimen* va individuato nella staticità che caratterizza l'ispezione a fronte della dinamicità dell'esperimento; quanto alla perizia, infine, la linea di confine appare più discutibile, perché coincide con il requisito delle "particolari cognizioni di scienze o arti", presente nella perizia ed assente nell'ispezione.

Più in dettaglio, l'art. 244, 1° comma, c.p.p. qualifica l'ispezione come lo strumento idoneo ad accertare su persone, cose o luoghi, "tracce" o "altri effetti materiali del reato". Solo nell'eventualità in cui il reato non abbia lasciato tracce o effetti materiali, ovvero quando questi siano stati "cancellati", "dispersi", "alterati", "rimossi", o comunque siano "scomparsi", il comma 2 del medesimo articolo prevede la possibilità, per l'autorità giudiziaria, di descrivere lo "stato attuale" di luoghi, cose o persone, indicando, ove possibile,

---

[185] Cfr. *Relazioni al progetto preliminare e al testo definitivo del codice di procedura penale*, cit., p. 59.
[186] Cfr. F. CORDERO, *Procedura penale*, Milano, 1991, p. 671; E. BASSO, *Commento agli artt. 244-246*, in *Commento al nuovo c.p.p.*, coordinato da M. CHIAVARIO, III, Torino, 1990, p. 676.
[187] Così, F. SIRACUSANO, *Manuale di procedura penale*, Milano, 1990, p. 373.
[188] Cass., sez. un., 3 luglio 1991, RIDPP, 1973, p. 903.
[189] C. PEYRON, *Ispezione giudiziale*, in *Enc. dir.*, XXII, Milano, 1972, p. 962.
[190] F. CORDERO, *Codice di procedura penale commentato*, cit., p. 281.

le "cause" delle modificazioni intervenute. Quindi, l'attività ispettiva consta di una prima fase, preliminare, di contatto tra l'organo procedente e le conseguenze materiali di un fatto di reato, ed una seconda successiva fase, consistente nella constatazione di una situazione "indiziante"[191]. Durante questa seconda fase dell'attività ispettiva, l'autorità può altresì disporre l'esecuzione di rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica si renda necessaria allo scopo.

In realtà, le norme del codice di rito non chiariscono esattamente in che cosa consista l'attività ispettiva. Gli art. 244 e ss. c.p.p. si limitano a stabilire il fine dell'attività di accertamento -distinguendo a seconda che si tratti di ispezione personale, locale o reale- senza alcuna pretesa definitoria, lasciando all'interprete il compito di dare un contenuto concreto a tale mezzo di ricerca della prova. Lo sforzo ermeneutico può giovarsi di due fondamentali fattori concorrenti: le "modalità di svolgimento" e le "finalità" caratterizzanti un'attività di accertamento definibile come di tipo ispettivo[192].

Quanto al primo aspetto, l'ispezione dovrebbe consistere in una mera percezione della realtà materiale, così come la stessa si presenta all'operatore, senza che si renda necessario un intervento modificatore di quest'ultimo. Si tratta, in altre parole, di una mera osservazione a carattere non modificativo della realtà di fatto (esseri umani, oggetti o luoghi) così come si presenta all'*inspiciens*[193]. Per specificare il contenuto dell'attività ispettiva in dottrina si è fatto riferimento in dottrina all'etimologia della parola "ispezione" che, come già detto, designa la ricerca visiva di un possibile segno[194], un'osservazione diretta ed immediata di persone, cose o luoghi[195]. In base ad una ulteriore opinione, peraltro, nell'ambito dell'attività ispettiva ben possono trovare collocazione anche forme di percezione della realtà esteriore diverse da quella visiva[196]: l'accertamento ispettivo, quindi, consisterebbe nella percezione, non solo visiva, della realtà materiale così come appare al soggetto attivo dell'ispezione.

---

[191] P. MOSCARINI, *Ispezioni (dir. proc. pen.)*, in *Enc. dir.*, Agg., II, Milano, 1998, p. 465.

[192] In questo senso, per un approfondimento, cfr. P. FELICIONI, *Le ispezioni e le perquisizioni*, in *Trattato di procedura penale*, diretto da G. UBERTIS e G.M. VOENA, Milano, 2012, p. 86.

[193] Cfr. C. BELLORA, *Ispezione giudiziale*, in *Dig. disc. pen.*, VII, Torino, 1993, p. 276; E. Basso, *Commento agli artt. 244-246,* cit., p. 673; L. CARLI, *Le indagini preliminari nel sistema processuale penale. Accusa e difesa nella ricerca e predisposizione delle prova penale*, II ed., Milano, 2005, p. 316; P. MOSCARINI, *Ispezioni (dir. proc. pen.)*, cit., p. 464.

[194] F. CORDERO, *Procedura penale*, 8^ ed., cit., p. 828.

[195] L. CARLI, *Le indagini preliminari nel sistema processuale penale*, cit., p. 316; P. MOSCARINI, *Ispezioni (dir. proc. pen.)*, cit., p. 464. V. PERCHINUNNO, *I mezzi di ricerca della prova*, in *Manuale di procedura penale*, Bologna, 2002, p. 244.

[196] Cfr. C. PEYRON *Ispezione giudiziale (dir. proc. pen.)*, cit., p. 962. Per la possibilità di usare qualunque senso (vista, udito, olfatto, tatto e gusto) a seconda della natura dell'oggetto dell'osservazione, cfr. G. LEONE, *Trattato*

Ciò in quanto -e veniamo al secondo aspetto- l'ispezione ha una finalità prevalentemente descrittiva, che si traduce nella mera enunciazione-narrazione degli elementi materiali (luoghi, cose, persone, sistemi informatici o telematici) che compongono la realtà di fatto e che si ritengono utili ai fini della ricostruzione del *lost fact.*

Sintetizzando, e cercando di tirare le fila del discorso, è possibile definire l'ispezione come «un mezzo di ricerca della prova tendente all'accertamento di elementi utili alla ricostruzione o alla verificazione del fatto affermato da una delle parti; si tratta di un accertamento che avviene tramite percezione diretta e descrizione delle entità materiali oggetto di osservazione»[197].

E' necessario distinguere, a questo punto, tra l'oggetto sul quale insiste l'attività di accertamento ispettivo e l'oggetto al quale è finalizzato l'accertamento medesimo. L'ispezione mira ad accertare le "tracce" e "gli effetti materiali del reato". La differenza fra tracce ed effetti è nota: le prime consistono in segni, macchie o impronte direttamente o indirettamente prodotte dalla condotta delittuosa su una determinata cosa o in un determinato luogo[198]; i secondi, invece, sembrano «richiamare alla mente le conseguenze o alterazioni di natura contundente, percussiva, ustionante, abrasiva, perforante, effrattiva che la stessa condotta può aver determinato su luoghi, cose o persone»[199]. Strumentale rispetto a questo fine è l'oggetto sul quale può vertere l'ispezione e cioè persone, cose, luoghi.

Ebbene, la legge 18 marzo 2008, n. 48, è intervenuta sull'ultima parte del 2 comma dell'art. 244, specificando che l'autorità giudiziaria può disporre rilievi «anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». Ergo, l'ispezione, ossia la osservazione finalizzata alla ricerca ed alla descrizione di tracce ed effetti del reato, ora può avere ad oggetto anche i dati digitali. Ma cosa significa ispezionare i dati digitali? In altre parole, in cosa consiste l'ispezione informatica e come si differenzia rispetto all'attiguo istituto della perquisizione informatica?

L'interrogativo si pone perché il medesimo documento informatico può essere oggetto di osservazione tramite ispezione, di ricerca attraverso la perquisizione e di apprensione mediante sequestro. In particolare, l'ispezione digitale consisterebbe in un'osservazione cui

---

di diritto processuale penale, II, Napoli, 1961, p. 189, e V. MANZINI, *Istituzioni di diritto processuale penale*, Padova, 1954, p. 156.

[197] Così, P. FELICIONI, *Le ispezioni e le perquisizioni*, cit., p. 88.

[198] Cfr. P.L. VIGNA, *Elementi di procedura penale per la polizia giudiziaria*, Roma, 2010, p. 80.

[199] Così, letteralmente, P. FELICIONI, *Le ispezioni e le perquisizioni*, cit., p. 89.

non segue l'acquisizione di dati: l'osservazione è finalizzata esclusivamente ad accertare la presenza di dati, informazioni e programmi all'interno di un determinato supporto[200].

In realtà, con riferimento al digitale le caratteristiche dell'accertamento che consentono di distinguere nettamente gli istituti tradizionali della ispezione, della perquisizione e del sequestro perdono significato. Infatti, osservare un *file* significa "mettere le mani" sul dispositivo di memorizzazione, quantomeno per verificarne la presenza, se non proprio per visualizzarne il contenuto, sicché in ambito informatico osservazione e ricerca sembrano avere il medesimo contenuto attuativo. Inoltre, esplorare un sistema alla ricerca di dati e tracce informatiche inerenti ai fatti oggetto dell'ispezione comporta irrimediabilmente l'alterazione dei dati di sistema o, comunque, la modifica dei metadati[201]. Senza contare che la copia-clone del *file* di interesse investigativo rinvenuto all'esito dell'attività di ricerca rende superfluo il sequestro del dato originale, al punto che in dottrina si parla di mancanza di attualità di quest'ultimo istituto processuale con riferimento al dato digitale[202].

Secondo alcuni studiosi che si sono occupati di questo fenomeno di "simbiosi" delle categorie processuali, la differenza tra ispezione e perquisizione si dovrebbe cogliere nei sistemi informatici in cui è possibile rinvenire dati coperti da credenziali di accesso e dati "liberi", cioè accessibili a qualsiasi utente abbia in uso quel determinato sistema: secondo tale opinione, rientrerebbe nell'ambito di un'attività ispettiva la visione dei *files* privi di password, mentre saremmo di fronte ad una perquisizione tutte le volte in cui la lettura del *file* richieda particolari sistemi di autenticazione[203].

Chi non condivide tale impostazione traccia la linea di confine tra ispezione e perquisizione molto prima della lettura del file contenuto nel sistema: in una *scena criminis*

---

[200] L. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in AA.VV., *Sistema penale e criminalità informatica*, Milano, 2009, p. 192.

[201] Un metadato (dal greco μετὰ "oltre, dopo" e dal latino *datum* "informazione" - plurale: data), letteralmente "(dato) oltre un (altro) dato", è un'informazione che descrive un insieme di dati. In informatica, ciascun file è portatore di dati (il suo contenuto) e metadati, come la sua data di creazione, la data di ultimo accesso e di modifica, il nome del suo autore, ecc.

[202] Cfr. E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenuto al contenitore, passando per la copia*, in *Cass. pen.*, 2010, p. 1533.

[203] «Il panorama si complica ulteriormente nel caso di utilizzo delle cd preview: attraverso l'utilizzo di software ad hoc viene permesso agli inquirenti in sede d'ispezione, ma anche di perquisizione (fattore, questo, che alimenta ulteriormente la "confusione applicativa" fra i due istituti), di poter analizzare in maniera grossolana il contenuto di un dispositivo per poi scegliere il materiale interessante e, se del caso, procedere a sequestro del dato. Si osserva, tuttavia, come tale operazione debba essere condotta da personale altamente qualificato, stante l'alto rischio di alterazione dei contenuti con conseguente dispersione di una possibile prova e, altresì, debba essere valutata caso per caso non rappresentando ad oggi operazione di routine applicabile indiscriminatamente a qualsiasi fattispecie concreta». Così, C. MAIOLI - E. SANGUEDOLCE, *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, www.altalex.com, 30 novembre 2015.

informatica, l'ispezione consiste nell'osservazione del sistema informatico o telematico, nella sua descrizione, nell'elenco delle periferiche collegate, nella specificazione di particolari sistemi hardware o software presenti, nella descrizione formale dell'eventuale sistema di connessione alla rete Internet[204]. Questa tipologia di attività -in apparenza poco utile- trova la sua ragion d'essere nella più approfondita considerazione secondo cui attualmente parlare di *scena criminis* informatica significa riferirsi non soltanto al tradizionale personal computer, ma anche a sempre più numerosi dispositivi mobili quali *smartphone*, *tablet*, ecc. Inoltre, rientrano sempre nell'ambito di una mera attività ispettiva i rilievi fotografici e le riprese video dello stato dei luoghi dove è allocato il sistema informatico o il *server*.

3.2. La perquisizione informatica

Il vocabolo "perquisizione" deriva dal latino *perquirere*, traducibile come attività di ricerca diligente[205]. Nel dettaglio, il verbo *quarere* indicherebbe l'attività di ricerca, mentre il suffisso *per* alluderebbe all'utilizzazione del corpo della persona o del luogo nello svolgimento dell'atto[206]. Il fine di tale attività di ricerca è quello di individuare ed apprendere il corpo del reato o cose pertinenti al reato[207].

In particolare, l'art. 247 c.p.p. prevede che le perquisizioni –personali o locali- possano essere disposte dall'autorità giudiziaria in quattro ipotesi: 1) quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato; 2) quando vi è fondato motivo di ritenere che il corpo del reto o le cose pertinenti al reato si trovino in un luogo determinato; 3) quando vi è fondato motivo di ritenere che in un luogo individuato si possa eseguire l'arresto dell'imputato o dell'evaso; 4) quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico (art. 247, comma 1-*bis*, c.p.p.)[208].

---

[204] «L'attività ispettiva in ambiente informatico dovrebbe limitarsi ad osservare il sistema descrivendolo nei suoi particolari, ad esempio rilevando la presenza di periferiche collegate, accesso alla rete attivo, presenza di software in funzione, partizioni logiche nascoste e rese visibili da meccanismi di autorizzazione connessi allo status dell'utilizzatore (ad esempio amministratore di sistema e chiavi di cifratura)». Così C. MAIOLI - E. SANGUEDOLCE, *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, www.altalex.com, 30 novembre 2015. Cfr., inoltre, S. Aterno, *Modifiche al titolo III del terzo libro del codice di procedura penale*, cit., pp. 206 e ss.

[205] F. CORDERO, *Procedura penale*, 8^ ed., cit., p. 832.

[206] Così, G. FOSCHINI, *Sistema del diritto processuale penale*, I, Milano, 1965, p. 72.

[207] P. FELICIONI, *Le ispezioni e le perquisizioni*, cit., p. 2.

[208] L'inserimento del comma 1-*bis* nel corpo dell'art. 247 c.p.p., come noto, si deve all'art. 8 della già citata legge 18 marzo 2008, n. 48.

Fondamentalmente, sono tre gli elementi che caratterizzano un'attività di perquisizione: la modalità di espletamento; la duplice finalità di tale mezzo di ricerca della prova; la coercizione, strumentale alla ricerca.

Quanto al primo aspetto, l'essenza della perquisizione consiste nella ricerca materiale di qualcosa di rilevante per il procedimento penale in corso, che preesiste rispetto al processo; la conseguenza è la corretta, anche se riduttiva, collocazione sistematica di tale istituto nell'ambito dei mezzi di ricerca della prova e non tra i mezzi di prova. La doppia, alternativa o cumulabile, funzione consiste nell'acquisizione di elementi probatori o nell'esecuzione di un provvedimento coercitivo personale. La coercibilità dell'attività di ricerca, infine, rientra a pieno titolo tra le deroghe previste dalle norme costituzionali che tutelano la libertà personale e domiciliare.

Al contrario dell'ispezione, la perquisizione postula un atteggiamento di "manomissione" dell'investigatore. Perquisire significa, cercare qualcosa, modificando lo stato dei luoghi: «si ha perquisizione […] quando l'investigatore non si limita alla mera osservazione delle particolarità di una persona, di un luogo o di un oggetto, ma si puntualizza in una ricerca accurata volta al rinvenimento del corpo del reato o delle cose ad esso pertinenti»[209]. E' tale tensione ad impossessarsi della cosa a caratterizzare la natura della perquisizione, prescindendo dallo strumento utilizzato dall'operatore (le mani o altri strumenti idonei a superare i propri limiti fisici).

Così come per l'ispezione, occorre distinguere tra l'oggetto della ricerca (corpo di reato o cose pertinenti al reato) e la realtà materiale sulla quale cade l'attività del perquirente. In particolare, all'indomani della modifica intervenuta con la già citata legge n. 48 del 2008, tale realtà può essere una persona, un luogo, ma anche un sistema informatico o telematico.

In ambito informatico, la perquisizione si traduce nella ricerca, all'interno del dispositivo, dei *file* di interesse investigativo. La ricerca presuppone, comunque la si voglia intendere, una "intrusione" all'interno del dispositivo. Ecco perché, con riferimento alla "cosa" digitale, la perquisizione deve necessariamente seguire l'apprensione (sequestro) del bene e non, viceversa, costituire attività prodromica al successivo eventuale sequestro[210].

---

[209] Così, P. FELICIONI, *Le ispezioni e le perquisizioni*, cit., p. 96.

[210] Di questa opinione, tra gli altri, L. LUPARIA, *La ratifica della Convenzione cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. I profili processuali*, cit., p. 720, nota 19 ed E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit., p. 154.

Si tratta dell'unico caso in cui la perquisizione segue il sequestro (o meglio, la copia) anziché precederlo, ed il motivo è presto detto: la ricerca si traduce inevitabilmente in un attività in grado di alterare il dato originale, sicché il suo espletamento deve avere ad oggetto la copia forense e mai l'originale, pena la violazione degli art. 247 e 352 c.p.p., così come modificati dalla riforma del 2008.

3.3. Il sequestro probatorio di dati digitali

La legge n. 48 del 2008 è intervenuta anche in tema di sequestro probatorio, interpolando il contenuto di diverse norme del codice di rito al fine di adeguarle alla nuova realtà dematerializzata. In particolare, l'art. 254 (sequestro di corrispondenza)[211] è stato aggiornato attraverso la previsione che gli oggetti di corrispondenza possono anche essere inviati per via "telematica" e la sostituzione dei vecchi «uffici postali» con la più attuale dicitura di «coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni». Al 2° comma della medesima disposizione si specifica, inoltre, che gli ufficiali di polizia giudiziaria che procedono al sequestro non solo non possono aprire gli oggetti di corrispondenza, ma neanche "alterarli". E' chiaro, qui, il riferimento alla corrispondenza digitale, ontologicamente esposta, per sua natura, al rischio di contaminazione. Inoltre, è stato inserito nel codice di rito l'art. 254-*bis*, con il quale si disciplinano le modalità del sequestro di dati informatici presso i fornitori dei servizi informatici, telematici e di telecomunicazioni. La disposizione prevede che l'autorità giudiziaria, nel disporre il sequestro dei dati, possa stabilire che l'acquisizione avvenga mediante copia su supporto informatico, «con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità». Emergono, quindi, le due esigenze fondamentali in tema di evidenze digitali: il dato deve essere *ab origine* genuino e successivamente non alterabile. Il fornitore dei servizi dovrà comunque attivarsi per conservare e proteggere adeguatamente i dati originali. Quanto al dovere di esibizione (art.

[211] L'articolo 254 c.p.p. prevede il sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza che possano costituire corpo di reato o che possano avere una qualche relazione con esso (spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa). Per la particolare tutela costituzionale che ha la corrispondenza, il codice ha voluto regolare tale ipotesi sia quando viene messa in atto dall'autorità giudiziaria, sia quando è di iniziativa della polizia giudiziaria. In quest'ultimo caso, ai sensi del comma 2, la corrispondenza dovrà essere consegnata all'autorità giudiziaria senza aprire gli oggetti o prendere altrimenti conoscenza del loro contenuto.

256 c.p.p.[212]), la legge del 2008 ha aggiunto che il sequestro può riguardare non solo gli atti e i documenti, ma anche «i dati, le informazioni e i programmi informatici», i quali possono essere sequestrati «mediante copia di essi su adeguato supporto». All'art. 259 c.p.p. (Custodia delle cose sequestrate)[213], comma 2, si è aggiunto un periodo volto a specificare che se la custodia riguarda dati informatici il custode deve essere anche avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi. *ex* art. 260 c.p.p. (Apposizione di sigilli alle cose sequestrate. Cose deperibili. Distruzione di cose sequestrate[214]) si è previsto l'onere di assicurare l'integrità delle cose di natura digitale sequestrate attraverso l'apposizione di sigilli di carattere elettronico o informatico, idonei ad indicare il vincolo imposto a fini di giustizia. Si ritiene che tale previsione rappresenti il recepimento, a livello processuale, della *best practice* relativa alla procedura di validazione della copia (certificazione della corrispondenza fra copia e originale) nota con il nome di funzione di hash. Inoltre, la eventuale copia dell'evidenza digitale (idonea ad evitare rischi di alterazione) deve essere realizzata su adeguati supporti mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità (comma 2).

I dispositivi di memorizzazione digitale delle informazioni possono rilevare sia come corpo del reato[215], sia come cose pertinente al reato[216]. Nel primo caso, il sequestro probatorio si sostanzia nell'apprensione fisica del dispositivo *hardware*. Nel secondo caso, invece, in base alle modifiche intervenute ad opera della legge n. 48 del 2008, il sequestro dovrebbe

---

[212] L'articolo 256 c.p.p., comma 1, prevede che i ministri di confessioni religiose, gli avvocati, gli investigatori privati autorizzati, i consulenti tecnici e i notai, i medici e i chirurghi, i farmacisti, le ostetriche e ogni altro esercente una professione sanitaria, gli esercenti altri uffici o professioni ai quali la legge riconosce la facoltà di astenersi dal deporre determinata dal segreto professionale, nonché i pubblici ufficiali, i pubblici impiegati e gli incaricati di un pubblico servizio debbano consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti e ogni altra cosa, salvo che dichiarino per iscritto che si tratti di segreto di Stato o di segreto inerente al loro ufficio o professione.

[213] Il quale dispone che le cose sequestrate siano affidate in custodia alla cancelleria o alla segreteria o, se ciò non è possibile, ad un altro custode (comma 1) che dovrà essere avvertito degli obblighi connessi alla custodia e delle pene previste per la violazione di tali obblighi (comma 2).

[214] L'articolo 260 c.p.p. descrive le attività materiali che vengono eseguite al fine di impedire che le cose sottoposte a sequestro vengano manipolate o ne venga modificato lo status quo. Ai sensi del comma 1, infatti, le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che le assiste oppure, in relazione alla natura delle cose, con altro mezzo idoneo a indicare il vincolo imposto a fini di giustizia. Come chiarisce la disposizione, infatti il sigillo non è il mezzo con il quale si assicura materialmente la intangibilità della cosa, ma è uno strumento simbolico attraverso cui si manifesta la volontà dello Stato diretta ad assicurare tali beni contro la manomissione. Se le cose oggetto di sequestro possono alterarsi, l'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni (comma 2) quindi, a seconda dei casi, ne ordina l'alienazione o la distruzione (comma 3).

[215] Tutte le volte in cui il dispositivo rappresenta l' "arma del delitto", ossia lo strumento attraverso il quale la condotta del soggetto agente pone in essere c.d. reati informatici puri.

[216] Ossia strumento per risalire, attraverso le tracce ivi presenti, alle fasi preparatorie e alla condotta assunta in concreto dal soggetto indagato.

tradursi nella effettuazione, ove possibile, di una "copia-clone" dei dati digitali contenuti nel dispositivo, attraverso una procedura idonea ad evitare alterazioni successive, sia dell'originale che della copia.

Quanto alla prima ipotesi, in un reato informatico puro possiamo qualificare giuridicamente come "corpo del reato" esclusivamente il *case* del sistema informatico e mai le sue periferiche. Di tal ché sarebbe inutile, oltreché errato, procedere al sequestro indiscriminato di stampanti, tastiere, schermi, mouse, ecc. Ciò che conta è l'elaboratore: «gli accessori non possono ritenersi rientranti nel concetto di corpo del reato, non essendo cose mediante le quali è stato commesso il reato»[217].

Nella seconda ipotesi il sequestro fisico cede il passo al sequestro logico di dati, che si realizza attraverso l'ormai nota *bit stream image*. In questo caso, i profili di criticità aumentano e la causa appare evidente: siamo nell'ambito di procedimenti penali per reati c.d. comuni dove il dispositivo di memorizzazione digitale rileva non in sé, come corpo del reato, bensì indirettamente, quale contenitore di informazioni rilevanti al fine di ricostruire il fatto storico. Il vincolo di pertinenzialità, quindi, riguarda i dati digitali e non i supporti ove questi sono memorizzati, con la conseguenza che è necessario distinguere, con tutte le difficoltà tecniche del caso, il contenitore dal contenuto, passando per la copia[218].

D'altronde, l'acquisizione di informazioni (*rectius* dati digitali) contenute all'interno della memoria di un computer non deve trasformare l'attività di indagine in un'attività di ricerca della *notitia criminis*; questa, infatti, deve precedere e non essere il risultato dell'espletamento del mezzo di ricerca della prova. Ciò significa evitare acquisizioni indiscriminate di dati digitali senza uno stretto vincolo di pertinenzialità rispetto al reato per cui si procede[219]. Sul punto si scontrano diverse esigenze: da un lato l'interesse pubblico all'acquisizione genuina di elementi utili per l'indagine nell'ottica della ricerca della verità processuale; dall'altro il diritto dell'indagato al rispetto della *privacy*, evidentemente lesa da un'acquisizione generalizzata di informazioni. Il giusto punto di equilibrio tra queste opposte esigenze è da rinvenire in un sequestro logico, il più possibile circoscritto ai dati di effettivo interesse

---

[217] Tribunale Riesame, Venezia, ord. 6 ottobre 2000. In dottrina, cfr. A. MONTI, *No ai sequestri indiscriminati di computer*, in *Diritto dell'Internet*, 3, 2007, pag. 268.

[218] Le parole sono di E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenuto al contenitore, passando per la copia*, cit., p. 1533.

[219] «L'atto acquisitivo, non individuando in maniera chiara e specifica il legame intercorrente fra il reato per cui si procedeva e l'azione di sequestro dell'intera memoria informatica, si è risolto in una acquisizione indiscriminata (…)», generando l'illegittimità del sequestro stesso. Così, A. LOGLI, *Commento alla sentenza n°753/2007*, in *Cass. pen.*, 7-8, 2008 pp. 2956-2957.

investigativo, il quale tuttavia non obliteri, pena l'inutilizzabilità, la genuinità della informazioni acquisite. Quindi, laddove sia tecnicamente impossibile procedere ad un'acquisizione mirata e genuina, è opportuno privilegiare il sequestro del contenitore, onde procedere successivamente alla selezione del materiale da acquisire in contraddittorio con la controparte, *ex* art. 360 c.p.p.

In ogni caso, oggetto del sequestro è il dato in sé, pur nella sua essenza dematerializzata, con la conseguenza che la restituzione del dispositivo non priva la parte del potere di contestare il sequestro, rimanendo in capo ad essa l'interesse ad impugnare il provvedimento. Premesso che «il dato informatico costituisce una realtà suscettibile di sequestro [..] la restituzione all'avente diritto del supporto su cui ne avviene la memorizzazione non fa venire meno il vincolo reale apposto su di esso». L'operazione di copia di un insieme di informazioni digitali non esclude, quand'anche sia restituita la loro fonte originaria, che esse siano sottratte al soggetto che ne disponeva. Il concetto stesso di copia perde di significato nel caso del documento informatico, in quanto il dato originale sarà perfettamente identico o, per meglio dire, sarà indifferentemente identico rispetto alla sua copia. L'interesse ad impugnare, quindi, sussiste anche quando il supporto fisico con i dati originali sia restituito al legittimo proprietario. Perciò, avverso il provvedimento di sequestro di una realtà digitale potranno dispiegarsi tutti i mezzi di impugnazione previsti dal codice. Ritenere il contrario, significherebbe accettare l'idea che un vincolo reale possa discendere da un provvedimento inoppugnabile, cosa, evidentemente, fuori da ogni possibile margine di sostenibilità.

4. Indagini tecniche su materiale digitale

Durante la fase delle indagini preliminari, il c.d. "potere tecnico" spetta indistintamente alla polizia giudiziaria, al pubblico ministero ed ai difensori delle parti private. In particolare, la polizia giudiziaria agisce "tecnicamente" a norma degli artt. 348 e 354, co. 2, c.p.p.[220]: in

[220] L'art. 348 c.p.p. (assicurazione delle fonti di prova) prevede espressamente la facoltà della polizia giudiziaria di compiere (di iniziativa o su delega del p.m.) atti o operazioni che richiedono specifiche competenze tecniche, avvalendosi dell'ausilio di persone idonee, il tutto al fine di assicurare le fonti di prova, cioè raccogliere ogni elemento utile alla ricostruzione del fatto ed alla individuazione del colpevole, ricercare le cose e le tracce pertinenti al reato nonché provvedere alla conservazione dello stato delle cose e dei luoghi. Più in dettaglio, il successivo art. 349 (identificazione della persona nei cui confronti vengono svolte le indagini e di altre persone) consente alla polizia giudiziaria di eseguire rilievi dattiloscopici, fotografici e antropometrici, nonché altri accertamenti" al fine di identificare l'indagato. L'art. 354 (accertamenti urgenti sui luoghi, sulle cose e sulle

questo caso, l'attività assume il "vestito giuridico" del "rilievo" o dell' "accertamento urgente". Al pubblico ministero, invece, sono dedicati gli artt. 359 e 360 c.p.p.: si tratta, come noto, degli "accertamenti tecnici", i quali a loro volta possono essere di natura ripetibile[221] o non ripetibile[222]. Al difensore, infine, la facoltà di effettuare indagini difensive di natura tecnica è riconosciuta *ex* artt. 391-sexies, 391-*septies* e 391-*decies* c.p.p. In base alla terminologia utilizzata dal legislatore[223], gli accertamenti qualificabili come "tecnici" sarebbero di esclusiva competenza della parti (pubblico ministero e difensori privati), le quali agiscono tramite propri consulenti, mentre alla polizia giudiziaria residuerebbe il potere-dovere di rilevare/accertare in situazioni di urgenza, a patto che tali operazioni non siano connotate da tecnicismo. Tale dicotomia è la conseguenza di una scelta, storicamente datata e forse ormai obsoleta, ben precisa: ripartire il "potere tecnico" tra i diversi soggetti processuali in base alle rispettive attribuzioni e competenze[224].

La domanda, a questo punto, sorge spontanea: alla luce del progresso tecnologico che caratterizza l'era digitale ha ancora senso oggi tale distinzione[225]? In particolare, con riferimento alle attività finalizzate al trattamento della prova informatica, è davvero possibile differenziare dal punto di vista tecnico l'attività della polizia giudiziaria rispetto a quella dei consulenti? La risposta, si anticipa, non può che essere negativa.

Argomentare tale conclusione significa necessariamente tornare sugli elementi distintivi che tradizionalmente insistono tra le attività di cui all'art. 354 c.p.p. e quelle descritte dall'360

---

persone. Sequestro) prevede la possibilità che la polizia giudiziaria possa compiere i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose se il pericolo che le cose le tracce e i luoghi si alterino, si disperdano comunque si modifichino e il pubblico ministero non sia intervenuto ovvero non abbia assunto la direzione delle indagini.

[221] A norma dell'art. 359 (consulenti tecnici del pubblico ministero), «il pubblico ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di consulenti, che non possono rifiutare la loro opera».

[222] *Ex* art. 360 c.p.p., in combinato disposto con l'art. 117 disp. att., la non ripetibilità può dipendere dall'oggetto («cose e luoghi il cui stato è soggetto a modificazione») o dalla modalità di svolgimento dell'accertamento (che «determina modificazioni delle cose, dei luoghi o delle persone tali da rendere l'atto non ripetibile»).

[223] Invero, tanta confusione in una materia così delicata è stata ingenerata dallo stesso legislatore che, in diversi articoli del codice, ha utilizzato lo stesso termine per indicare attività differenti: accertamenti, per la polizia giudiziaria; accertamenti tecnici per gli altri.

[224] Cfr. M. CONTE – R. LONFORTI, *Gli accertamenti tecnici nel processo penale*, Milano, 2006; L. - P. L. VIGNA, *La pratica di polizia giudiziaria, I, La polizia giudiziaria nel processo penale*, VII ed., Padova, 2007; Id., *Pratica di polizia giudiziaria,* Padova, 2012. Per un esame completo delle norme del codice di rito dove è possibile constatare letteralmente tale distinzione in termini lessicali, cfr. G. ICHINO, *L'attività di polizia giudiziaria*, in AA.VV., *Indagini preliminari ed instaurazione del processo*, a cura di M. G. AIMONETTO, Torino, 1999, p. 181.

[225] Ne dubita, tra gli altri, A. SCALFATI, *La deriva scientista dell'accertamento penale*, in *Proc. pen. giust.*, 2011, n. 5, p. 148.

c.p.p. All'esito di tale preliminare operazione, occorre calarsi all'interno della categoria dei rilievi e degli accertamenti urgenti, onde qualificare i concetti di "urgenza" e "necessità", al precipuo scopo di chiarire i presupposti legittimanti l'intervento unilaterale su materiale informatico.

4.1 Il superamento della tradizionale distinzione tra rilievi e accertamenti tecnici

A mente dell'art. 354, co. 1, c.p.p., «Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero». Il successivo comma 2, precisa che «Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. […] Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti». La disposizione in commento prevede quindi un complesso di attività atipiche finalizzate, pur nella ricerca, alla conservazione ed all'assicurazione di tutto ciò che può essere utile alla ricostruzione del fatto di reato. In particolare, è possibile distinguere tre tipologie di attività[226]: 1) una prima attività di congelamento della scena del crimine, che si attua ad esempio attraverso la delimitazione del luogo e l'allontanamento dei "non addetti ai lavori"; 2) una seconda fase in cui vengono espletate le operazioni tecniche di osservazione e descrizione di tutti gli elementi utili ai fini delle indagini; 3) un'ultima fase di repertazione. Si tratta di osservare, percepire, individuare ed acquisire le tracce e gli effetti materiali del reato, tutte operazioni che rientrano in quella funzione, tipica della polizia giudiziaria, essenzialmente "narrativa", materiale e preparatoria rispetto alla consulenza che il pubblico ministero potrebbe in seguito predisporre[227]. Tale attività può avere ad oggetto fonti di prova reale[228] o

---

[226] Cfr. P. FELICIONI, *Le ispezioni e le perquisizioni*, cit., p. 427. Certo è che sin dal primo accesso alla scena del crimine il lavoro degli inquirenti si prefigge non solo di indirizzare le indagini, ma anche e soprattutto di «svolgere una proficua attività proiettata nell'ottica dibattimentale». Così, SOTTANI, *Rilievi e accertamenti sulla scena del crimine*, in *Arch. pen.*, 2011, 3, 1.

[227] Cfr. SOTTANI, *Rilievi e accertamenti sulla scena del crimine*, cit., p. 4; E. APRILE, *Le indagini tecnico-scientifiche: problematiche giuridiche sulla formazione delle prova penale*, in *Cass. pen.*, 2003, p. 4036. Cfr., inoltre, L. D'AMBROSIO – P. L. VIGNA, *La pratica di polizia giudiziaria*, cit., p. 221, dove si legge che i rilievi e gli accertamenti urgenti di cui al comma 2 dell'art. 354 svolgono un ruolo "espositivo" e "propedeutico" rispetto al momento valutativo che caratterizza i successivi accertamenti tecnici. In questo senso, anche DE LEO, *Le indagini tecniche di polizia: un invito al legislatore*, in *Cass. pen.*, 1996, p. 697, nonché SCELLA, *Brevi*

personale[229] e può avere come conseguenza il sequestro del corpo del reato e delle cose ad esso pertinenti. Le condizioni qualificanti l'urgenza e legittimanti l'intervento unilaterale della polizia giudiziaria sono due: il c.d. *periculum in mora*, ossia il pericolo che nel frattempo lo stato dei luoghi cambi o le tracce vadano perdute e l'impossibilità di un tempestivo intervento del pubblico ministero o la mancata assunzione della direzione delle indagini da parte dello stesso[230]. Si tratta di situazioni nelle quali un ritardo nell'azione potrebbe compromettere in modo irreversibile lo *status quo* a causa dell'agire degli agenti atmosferici o della necessità di rendere sicura la scena del crimine o anche come conseguenza del naturale deterioramento che connota gli elementi di tipo organico[231]. E' chiaro che non intervenire in situazioni del genere significherebbe rinunciare per sempre alla possibilità di identificare potenziali sospettati o alla opportunità di ricostruire correttamente la dinamica degli eventi. Tale dev'essere la spiegazione del contenuto composito dell'art. 354, archetipo delle attività ad iniziativa della polizia giudiziaria. *Nulla quaestio* circa le attività di tipo informativo e conservativo, ma di natura "passiva"; maggiori problemi, a livello interpretativo, desta quell'attività cautelativa "attiva" che si concretizza in «rilievi e accertamenti sullo stato dei luoghi e delle cose»[232]: *conditio sine qua non* del loro espletamento dovrebbe essere la loro attitudine a «non causare la distruzione o l'inservibilità del reperto oggetto d'intervento, come conferma l'art. 117 disp. att., imponendo –per l'accertamento che determini 'modificazione delle cose, dei luoghi o delle persone tali da rendere l'atto non [riproducibile]' l'adozione della procedura prevista dall'art. 360 c.p.p.»[233]. Si tratta pur sempre di attività dotate di una forte carica probatoria, tali da essere inserite direttamente nel fascicolo per il dibattimento ai sensi dell'art. 431, comma 1, lett. b, del codice di procedura penale, ed essere lette in dibattimento (ex art. 511 c.p.p.). Di conseguenza, il sistema ha controbilanciato questo dominio probatorio con un articolato di cautele a beneficio dell'imputato: l'art. 357, comma 2,

---

riflessioni in tema di accertamenti tecnici, rilievi e tutela del diritto di difesa, in *Cass. pen.*, 1990, p. 278 e L. D'AMBROSIO, *Pratica di polizia giudiziaria*, Padova, 2012, p. 158.

[228] Cfr. G. ICHINO, *L'attività di polizia giudiziaria*, cit., p. 131.

[229] A condizione che tali attività non si traducano in vere e proprie ispezioni personali, di esclusiva competenza dell'autorità giudiziaria a norma dell'art. 244 c.p.p. Cfr. L. LUPARIA, *Attività d'indagine a iniziativa della polizia giudiziaria*, in G. GARUTI (a cura di), *Indagini preliminari e udienza preliminare*, in *Trattato di procedura penale*, G. SPANGHER (diretto da), vol. III, Torino, 2009, p. 225.

[230] V. P. TONINI, *Manuale di procedura penale*, cit., p. 516.

[231] V. LUPARIA, *Attività d'indagine a iniziativa della polizia giudiziaria*, cit., p. 222.

[232] E' appena il caso di notare che i termini "rilievi" e "accertamenti" vengono usati dal legislatore nell'art. 354, co. 2, c.p.p. in modo a-tecnico, quasi come se fossero sinonimi. Non importa in questa sede scandagliare le possibili differenze tra questi due atti, ciò che conta è che entrambi sono di spettanza della polizia giudiziaria al sussistere dell'urgenza qualificata dalla norma.

[233] Così, L. LUPARIA, *Attività d'indagine a iniziativa della polizia giudiziaria*, cit., p. 224.

lett. e, del codice di procedura penale, contempla l'obbligo di documentazione delle azioni svolte tramite specifico verbale; l'art. 356 del codice di procedura penale consente al difensore di assistere agli accertamenti, pur senza il diritto di essere preventivamente avvisato[234]; l'art. 366 del codice di procedura penale impone alla polizia giudiziaria l'onere di depositare gli atti nella segreteria del pubblico ministero entro il terzo giorno successivo al loro compimento, con facoltà per i difensori di esaminarli ed estrarne copia nei cinque giorni successivi.

L'art. 360 c.p.p., come noto, è dedicato ai c.d. "accertamenti tecnici irripetibili" che, «incastonati, anch'essi, nel più ampio contesto di *screening* e accaparramento delle fonti di prova, rappresentano uno dei meccanismi indispensabili per intercettare elementi conoscitivi che, per le loro prerogative, esigono di avvalersi di soggetti dotati di particolari cognizioni tecniche, i c.d. consulenti tecnici»[235]. In base alla norma in commento, avvalendosi dell'opera di esperti il pubblico ministero è legittimato ad espletare operazioni tecniche di tipo specialistico su persone, cose o luoghi il cui stato è soggetto a modificazione, "bypassando" la necessità di ricorrere ad incidente probatorio, a patto che sussista l'urgenza del provvedere, nel senso che l'inerzia provocherebbe la dispersione della prova[236]. In questo caso, l'organo dell'accusa ha l'onere di preavvisare la persona sottoposta alle indagini, l'offeso e i difensori del conferimento dell'incarico, nonché della facoltà di nominare consulenti tecnici di parte. *ex* art. 117 disp. att., tale meccanismo procedurale si applica anche nell'ipotesi in cui gli accertamenti da eseguire siano suscettibili di alterare essi stessi l'oggetto dell'accertamento[237]. L'essenza dell'attività, in questo caso, consiste nello studio e nell'elaborazione valutativa, su

---

[234] Di questa facoltà la polizia giudiziaria ha il dovere di dare notizia all'indagato se presente (*ex* art. 114 disp. att. c.p.p.).

[235] Testualmente, O. BRUNO, *L'esaltazione di un'impronta digitale non configura un'ipotesi di accertamento tecnico irripetibile*, in *Proc. pen. giust.*, 2013, 5, p. 54. Per un approfondimento di tale strumento, cfr. M. CONTE - R. LOFORTI, *Gli accertamenti tecnici nel processo penale*, Milano, 2006.

[236] Cfr. C. BONZANO, *Attività del pubblico ministero*, in G. GARUTI (a cura di), *Indagini preliminari e udienza preliminare*), in *Trattato di procedura penale*, diretto da G. SPANGHER, vol. III, Torino, 2009, p. 315, secondo il quale sussiste «un pieno diritto della difesa a che gli accertamenti non ripetibili vengano svolti ad opera di un perito (nominato dal giudice e gravato dall'obbligo penalmente sanzionato di verità), nell'indicente probatorio, e dunque con la garanzia del contraddittorio, in condizioni di parità con l'accusa».

[237] Si tratta dei c.d. accertamenti modificativi o distruttivi. A tal proposito, cfr. G. CONTI – A. MACCHIA, *Indagini preliminari*, in *Enc. giur.*, XVI, Roma, 1989, p. 7. In generale, sul tema degli accertamenti tecnici non ripetibili cfr. G. SPANGHER, *La pratica del processo penale*. *Indagini preliminari e udienza preliminare. Il giudizio. Il procedimento davanti al Tribunale in composizione nonocratica*, vol. II, Padova. 2012, pp. 101 e ss.; C. BONZANO, *Attività del pubblico ministero*, cit., pp. 315 e ss.; P. GAETA, *sub art. 360 c.p.p.*, in *Codice di procedura penale commentato*, GIARDA-SPANGHER (a cura di), II, Milano, 2010, pp. 4346 e ss.; F. GIUNCHEDI, *Accertamenti tecnici*, in *Dig. pen.*, V agg., Torino, 2010, pp. 1 e ss.; Id., *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, Torino, 2009; L. GRILLI, *Le indagini preliminari della polizia giudiziaria e del pubblico ministero*, Padova, 2012, pp. 206 e ss..

base tecnica, degli elementi raccolti[238]. Il presupposto legittimante il ricorso a tale strumento normativo, anziché a quello più garantista dell'incidente probatorio, è l'urgenza qualificata in termini di "non utile ripetibilità" dell'accertamento, criterio discriminante tra prova legittima basata su un contraddittorio debole (accertamento tecnico non ripetibile, *ex* art. 360 c.p.p.) e prova formata attraverso un contraddittorio forte, ove le parti si trovano ad interloquire in condizioni di effettiva parità (in caso di incidente probatorio)[239].

Secondo la consolidata giurisprudenza di legittimità[240], si definiscono "rilievi"[241] tutte quelle attività materiali di raccolta, rilevamento e constatazione di elementi utili alla ricostruzione dei fatti oggetto del *thema probandum.* Si tratta di attività che non comportano una componente valutativa apprezzabile ed in questo si contrappongono agli "accertamenti

---

[238] Cfr. O. BRUNO, *L'esaltazione di un'impronta digitale non configura un'ipotesi di accertamento tecnico irripetibile*, cit., p. 55.

[239] Sul concetto di "non ripetibilità" le idee in dottrina sono molte. Ne dà atto, fra gli altri, O. BRUNO, *L'esaltazione di un'impronta digitale*, ult. op. cit., p. 55, la quale sottolinea che si va dalla «non utile rinviabilità» alla «indifferibilità» e alla «non rinnovabilità», sino a giungere al concetto di «impossibilità di ripetibilità in condizioni omogenee»; Cfr. V. BASSI, *Alcune riflessioni in materia di atti irripetibili alla luce della novella n. 356/92*, in *Cass. pen.*, 1994, pp. 2112 e ss., secondo il quale non rinviabili sono quegli atti «la cui assunzione risulta obiettivamente urgente ed indifferibile, stante il concreto rischio di modificazione inevitabile della situazione di fatto oggetto della prova o di sopravvenienza di condizioni che possono incidere sulla acquisizione o sulla genuinità dell'esame dibattimentale del soggetto fonte di prova. In questi casi l'irripetibilità dell'atto è, almeno in astratto, assoluta per il presumibile sopravvenire di cause oggettive e soggettive suscettibili di pregiudicare irrimediabilmente l'acquisizione e la genuinità dell'atto utilizzabile come prova ai fine del giudizio»; M. D'ANDRIA, *Un tentativo di definizione degli atti non ripetibili*, in *Cass. pen.*, 1992, pp. 1350 e ss., accosta la non ripetibilità alla non rinviabilità: «irripetibile, quindi, deve essere considerato ogni atto essenzialmente ricognitivo di situazioni obiettive sottoposte ad immediati processi di modificazione e non più riproponibili nello stesso contesto e con le stesse caratteristiche e modalità». MANZIONE, *L'attività del pubblico ministero. Indagini preliminari e instaurazione del processo*, coordinato da M. G. AIMONETTO, in *Giurisprudenza sistematica di diritto processuale penale*, diretta da M. CHIAVARIO - E. MARZADURI, Torino, 2009, p. 268, sostiene che vi sono «due concetti di irripetibilità, l'uno coincidente con l'indifferibilità, l'altro con la non rinnovabilità dell'atto […], sebbene a rigore in quest'ultimo caso non è il risultato dell'atto a venire in gioco quanto, piuttosto, la sua stessa esistenza […]. In definitiva, peraltro, entrambe le categorie sopra individuate hanno un comune denominatore nella non procrastinabilità dell'atto o, se si preferisce, nella sua non rinviabilità al dibattimento […].

[240] In giurisprudenza, cfr. Cass., sez. V, 20 novembre 2000, D'Anna, in *CED Cass.*, n. 218642; Cass., sez. II, 27 ottobre 1998, Bettio, *ivi*, n. 213311; Cass., sez. III, 19 gennaio 1995, Pezzantini, in *Cass. pen.*, 1997, p. 445; Cass., sez. II, 10 novembre 1992, Arena, in *CED Cass.*, n. 192570; Cass., sez. I, 9 febbraio 1990, Duraccio, in *Cass. pen.*, 1990, p. 278. In dottrina, cfr. L. D'AMBROSIO - P. L. VIGNA, *La pratica di polizia giudiziaria*, cit., p. 253; G. ICHINO, *L'attività di polizia giudiziaria*, cit., p. 183; R. E. KOSTORIS, *I consulenti tecnici nel processo penale*, Milano, 1993, p. 141; M. VESSICHELLI, *Sulla possibilità della p.g. di effettuare di propria iniziativa raffronti tra impronte digitali*, in *Cass. pen.*, 1992, p. 689; A. SCALFATI, *Gli accertamenti tecnici dell'accusa*, in *Indice pen.*, 1992, p. 129; A. SCELLA, *Brevi riflessioni in tema di accertamenti tecnici, rilievi e tutela del diritto di difesa*, cit., p. 278; P. P. DELL'ANNO, *Accertamento e valutazione nelle attività di consulenza disposte dal pubblico ministero*, in *Giust. pen.*, 1991, p. 241.

[241] Etimologicamente, la parola "rilievo" deriva dal latino *relevare*, ossia sollevare, ed è composta dal termine *levare*, cioè alzare, preceduto dal prefisso *re*, che sta ad indicare un movimento verso l'alto. Quindi, il suo esatto significato dovrebbe essere "togliere da terra" un qualcosa che già di per sé si distingue dal resto delle cose per caratteristiche sue proprie. «[U]tilizzata nel senso di attività di rilevamento, essa fa riferimento all'atto del cogliere elementi che effettivamente sporgono». Così, A. CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, cit., p. 78.

tecnici"[242], i quali consistono in attività di studio, analisi ed elaborazione valutativa dei dati precedentemente rilevati: «il rilievo tecnico consiste nell'attività di raccolta di elementi attinenti al reato per il quale si procede, mentre l'accertamento tecnico, ripetibile o irripetibile, si estende al loro studio e alla loro valutazione critica, secondo canoni tecnici, scientifici ed ermeneutici»[243]. Quindi, osservazione, cristallizzazione e, semmai, prelievo, da una parte; riflessione, apprezzamento e valutazione, dall'altra[244].

Tale distinzione serviva, tradizionalmente, per distinguere poteri e attribuzioni. Secondo l'intenzione del legislatore del 1988, la polizia giudiziaria doveva avere un compito prettamente cautelativo, di tipo conservativo, di tal ché al sussistere dell'urgenza era giustificata ed anzi doverosa l'effettuazione di rilievi ed accertamenti sui luoghi, sulle cose e sulle tracce pertinenti al reato: *nulla quaestio*, sulla unilateralità, peraltro fisiologica, di un simile intervento; d'altronde, non si ravvedeva alcun *vulnus* rispetto alle garanzie difensive della persona sottoposta alle indagini, dal momento che nessuna alterazione dello *status quo* poteva ragionevolmente scaturire da una semplice e materiale attività di raccolta di elementi indiziari. Il pubblico ministero e, in parallelo, i difensori privati, per mezzo dei rispettivi consulenti, avevano un più ampio e preciso potere di accertamento tecnico sui luoghi, sulle cose e sulle tracce pertinenti al reato, attività, quest'ultima, in grado di incidere essa stessa sulla genuinità degli elementi di prova: da qui, una più precisa e dettagliata disciplina delle diverse garanzie partecipative spettanti alla controparte in ipotesi di accertamenti tecnici ripetibili o non ripetibili.

Tutto ciò appare oggi anacronistico ed obsoleto. La scientificità del metodo pervade l'investigazione, a qualunque livello. Con specifico riferimento alla prova informatica diventa difficile immaginare un rilievo scevro da valutazioni di tipo tecnico, ovvero un accertamento tecnico che non sia preceduto da un rilievo dotato di altrettanto tecnicismo. In ambito digitale, anche la semplice "raccolta" del dato presuppone una elevata competenza ed una precisa specializzazione, perché richiede delle valutazioni di tipo tecnico circa le metodologie da utilizzare, il software da applicare, l'hardware da impiegare per raggiungere lo scopo imposto

---

[242] "Accertare", invece, viene da "certo", che a sua volta deriva dal latino *cernere*, che significa separare, distinguere, un qualcosa che di per sé rimarrebbe altrimenti indistinto (in assenza di accertamento).

[243] Cfr. Cass. pen. Sez. I, 30 aprile 2015, n. 18246 e Cass. pen., sez. II, 10 luglio 2009, n. 34149, Chiesa e altro, Rv. 244950.

[244] Tradizionalmente, la distinzione tra rilievi e accertamenti tecnici si basa sul seguente ragionamento: sarebbe attività di mero rilievo quella attraverso la quale, seppur con l'ausilio di mezzi tecnici, ci si limita ad individuare e raccogliere l'elemento di prova (attività materiale di cristallizzazione); costituirebbe, invece, attività di accertamento tecnico la successiva operazione di analisi e di valutazione dell'elemento raccolto (attività di rielaborazione di dati in precedenza acquisiti).

ex lege, ossia la tutela dei dati originali. In questo senso, si può allora sostenere che in ambito digitale il rilievo nasconda in realtà un accertamento tecnico o, se si preferisce (ma è lo stesso), che la distinzione tra rilievo e accertamento tecnico, quantomeno in ambito informatico, non abbia alcun senso[245].

D'altronde, etimologicamente la parola "rilievo" deriva dal latino *relevare*, ossia sollevare, ed è composta dal termine *levare*, cioè alzare, preceduto dal prefisso *re*, che sta ad indicare un movimento verso l'alto. Quindi, il suo esatto significato dovrebbe essere "togliere da terra" qualcosa che già di per sé si distingue dal resto delle cose per caratteristiche sue proprie[246]. "Accertare", invece, viene da "certo", che a sua volta deriva dal latino *cernere*, che significa separare, distinguere, qualcosa che in assenza di accertamento rimarrebbe indistinto. Ebbene, anche da questo punto di vista l'attività forense di estrazione di dati sembrerebbe senz'altro più simile ad un accertamento piuttosto che ad un rilievo.

Per ovviare a tale problema, una parte della dottrina parla più correttamente di rilievi con riferimento a quelle attività nelle quali la componente valutativa, pur esistente, caratterizza il metodo operativo di raccolta dei dati, mentre riserva la qualifica di accertamenti tecnici a quegli atti nei quali la valutazione si traduce in una rielaborazione critica dei dati acquisiti[247]. Secondo questa teoria, la vera differenza tra rilevare ed accertare non sta nella presenza o nell'assenza dell'aspetto tecnico-valutativo, quanto piuttosto nella diversa fase in cui esso rileva: nei rilievi, la valutazione tecnica attiene alle modalità con le quali, prudentemente, deve essere effettuato l'accertamento; negli accertamenti tecnici, il tecnicismo insiste sul risultato, che rappresenta il frutto di una valutazione. Seguendo tale ragionamento, l'estrazione delle copia forense rappresenta un tipico esempio di attività caratterizzata indubbiamente da aspetti tecnici-valutativi che, tuttavia, non riguardano il risultato, ma il metodo prescelto al fine di salvaguardare l'integrità dei dati digitali.

Senonché, una simile argomentazione, seppur condivisibile in linea teorica, non risolve il problema. Ed infatti, scomporre le fasi dell'attività investigativa onde arrivare a sostenere che

---

[245] «Importa poco cosa avesse in mente il legislatore delegato del 1988 quando elaborò quel nugolo di norme deputate a regolamentare la fase di ricerca ed assicurazione delle fonti di prova. Qualsiasi idea lo avesse ispirato, oggi risulta obsoleta e scantonata in un passato normativo molto più lontano della sua effettiva dimensione temporale. In pochi anni, tanto da non poterli contare che su due mani, la scienza e la tecnologia hanno fatto capolino nell'accertamento penale, anche nella fase del sopralluogo giudiziaria, penetrando con forza nei suoi metabolismi genetici». Così, D. CURTOTTI NAPPI E L. SARAVO, *L'approccio multidisciplinare nella gestione della scena del crimine*, in *Dir. pen. proc.*, 2011, 5, p. 623.

[246] «[U]tilizzata nel senso di attività di rilevamento, essa fa riferimento all'atto del cogliere elementi che effettivamente sporgono». Così, A. CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, cit., p. 78.

[247] *Ibidem*, p. 55.

al fine di qualificare come accertamento tecnico una determinata attività la valutazione rileva esclusivamente in sede di presentazione dei risultati equivale ad aggirare l'ostacolo, senza tuttavia risolverlo. Il punto è che in ambito digitale la precedente e propedeutica fase di raccolta degli elementi da valutare è parimenti, se non maggiormente, importante rispetto alla successiva fase di analisi forense, al punto che un errore commesso in fase di estrazione è in grado di minare l'attendibilità o, addirittura, l'utilizzabilità dell'evidenza digitale ottenuta. L'approccio investigativo ad una *scena criminis* informatica non è fatto di improvvisazione ed intuito, ma, sempre più spesso, di scienza e tecnica, le quali impongono un protocollo indefettibile.

Questo ci porta a dire che il difficile rapporto tra scienza e diritto processuale penale non riguarda solo la fase di valutazione e/o validazione della legge scientifica in giudizio, ma, più in generale, il rapporto tra scienza e procedimento penale in tutte le fasi in cui la prima entra in contatto con il secondo a scopo forense. La tecnologia informatica acuisce i già noti problemi tra scienza e processo[248], anticipandone la portata nella fase delle indagini preliminari e, in particolare, facendoli emergere in maniera dirompente durante il primo contatto dell'investigatore con la *scena criminis*. In questo nuovo contesto, il sopralluogo di polizia giudiziaria rappresenta il nuovo «nodo da sciogliere nel difficile rapporto tra scienza e processo penale»[249], in una fase, quella delle indagini preliminari, dove la regola è il segreto e in un momento, quello del sopralluogo giudiziario, dove il contraddittorio è solamente eventuale e posticipato.

4.2 Rilievi e accertamenti urgenti su materiale digitale: per una corretta interpretazione della loro "necessarietà"

Di regola, la polizia giudiziaria è il primo soggetto che interviene sulla *scena criminis* realizzando il primo contatto con le fonti di prova. Ciò, evidentemente, è espressione dell' *id*

---

[248] Cfr., per degli scritti recenti sul tema, M. BARGIS, *Note in tema di prova scientifica nel processo penale*, in *Riv. dir. proc.*, 2011, pp. 47 e ss.; C. CONTI, *Il processo si apre alla scienza. Considerazioni sul procedimento probatorio e sul giudizio di revisione*, in *Riv. it. dir. proc. pen.*, 2010, pp. 1204 e ss.; S. LORUSSO, *Investigazioni scientifiche, verità processuali ed etica degli esperti*, in *Dir. proc. pen.*, 2010, pp. 1345 e ss.; P. TONINI, *Informazioni genetiche e processo penale ad un anno dalla legge*, *ivi*, 2010, pp. 883 e ss.; Id., *La prova scientifica*, in *Trattato di procedura penale*, AA.VV., diretto a G. SPANGHER, vol. II, t. 1, *Le prove*, a cura di A. SCALFATI, Torino, 2009, pp. 88 e ss.; G. CANZIO, *Prova scientifica, ragionamento probatorio e libero convincimento del giudice*, in *Dir. pen. proc.*, 2003, p. 1194.

[249] Così, D. CURTOTTI NAPPI - L. SARAVO, *L'approccio multidisciplinare nella gestione della scena del crimine*, cit., p. 623.

quod plerumque accidit in un sistema processuale in cui a tale organo investigativo si assegna la funzione di «prendere notizia dei reati, impedire che vengano portati a conseguenze ulteriori, ricercarne gli autori, compiere gli atti necessari per assicurare le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della legge penale» (art. 55, co. 1, c.p.p.).

La polizia giudiziaria, intervenuta sul luogo dove è stato commesso il reato, deve «curare che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero» (art. 354, co. 1, c.p.p.), il quale deve essere informato «senza ritardo» (art. 347, co. 1, c.p.p.) dell'avvenuta acquisizione della notizia di reato. Anche dopo tale tempestiva informativa, la polizia giudiziaria deve raccogliere «ogni elemento utile alla ricostruzione del fatto e alla individuazione del colpevole» procedendo, fra l'altro «alla ricerca delle cose e delle tracce pertinenti al reato nonché alla conservazione di esse e dello stato dei luoghi» (art. 348, co. 1 e 2, c.p.p.).

Quindi, il primo e fondamentale compito della polizia giudiziaria consiste nella "conservazione" dello *status quo*, al fine di evitare la dispersione delle tracce e delle cose pertinenti al reato. Ad esempio, la polizia giudiziaria può circoscrivere il luogo del delitto, impedendo l'accesso a terzi e svolgendo attività di sorveglianza per evitare la sottrazione di elementi rilevanti o, comunque, l'alterazione dello stato dei luoghi. Peraltro, tale attività, necessariamente atipica, può comportare anche la effettuazione di accertamenti e rilievi, nonché il sequestro, di iniziativa, del corpo del reato e delle cose ad esso pertinenti, «se vi è il pericolo che le cose, le tracce e i luoghi pertinenti al reato si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente» (art. 354, co. 2, c.p.p.). Per la polizia giudiziaria, l'urgenza legittima dunque, oltre alla conservazione, anche la possibilità di compiere sulla scena del crimine atti di indubbia valenza investigativa e probatoria.

Il legislatore individua il fine della conservazione, ma non i mezzi per raggiungere tale scopo, cosicché l'attività di polizia giudiziaria finalizzata ad evitare manipolazioni e inquinamenti della *scena criminis* originaria può essere svolta in piena libertà di forma, purché idonea allo scopo[250]. Anche gli atti destinati ad avere valenza probatoria –rilievi e

[250] Cfr. Cass., sez. I, 4 maggio 1994, Ferraro, in *Giust. pen.*, 1995, III, c. 479; Cass., sez. III, 30 luglio 1994, Zanazzo, in *CED Cass.*, n. 199417. In dottrina, v. G. TRANCHINA, *Le attività della polizia giudiziaria nel procedimento per le indagini preliminari*, in D. SIRACUSANO – A. GALATI – E. ZAPPALÀ (a cura di), *Diritto processuale penale*, II, Milano, 2011, p. 97.

accertamenti- sono sicuramente atipici, anche se tipica è la situazione di urgenza che li giustifica: 1) modificazione inevitabile delle cose o dei luoghi dovuta al semplice trascorrete del tempo; 2) impossibilità di un tempestivo intervento del pubblico ministero[251]. In altre parole, al sussistere dei presupposti normativi qualificanti la situazione di urgenza, la polizia giudiziaria ha piena libertà organizzativa sia di ricerca, sia di assicurazione e conservazione delle tracce, delle cose e dei luoghi pertinenti al reato. La necessaria atipicità di tale attività è fuori discussione ed emerge sin dalla Relazione al progetto preliminare del codice del 1988, ove traspare la volontà di non vincolare la polizia giudiziaria[252], lasciandola libera di muoversi all'interno di una cornice di legittimità i cui contorni, tuttavia, meritano di essere precisati.

In particolare, il nodo problematico da sciogliere è il seguente: a fronte di tale incontestata atipicità, quali sono gli accertamenti e i rilievi urgenti che la polizia giudiziaria può legittimamente effettuare durante il primo accesso sul luogo del delitto e quali sono, invece, quelli che le sono preclusi? In altre parole, si tratta di calcolare l' "area" di legittimità dell'attività unilaterale urgente di polizia giudiziaria, destinata ad avere rilevanza investigativa e probatoria nel corso del processo. Ebbene, volendo utilizzare una metafora geometrica potremmo dire che la "base" e l' "altezza" del "rettangolo" degli atti urgenti sono rappresentate, rispettivamente, dall' "urgenza" e dalla "ripetibilità". Sicché, dalla combinazione di queste due misure dipende la vastità dell'aera di legittimità dell'atto unilaterale posto in essere dalla polizia giudiziaria in sede di sopralluogo *ex* art. 354, co. 2, c.p.p. Con la seguente precisazione: in una *scena criminis* informatica l' "urgenza" è in *re ipsa*, rimanendo dunque una sola variabile, la ripetibilità o meno dell'atto.

In ambito digitale, a parere di chi scrive e con buona pace della quasi unanime giurisprudenza, la risposta all'iniziale interrogativo (area di legittimità dell'intervento urgente di polizia giudiziaria) non passa attraverso la tradizionale distinzione tra rilievi e accertamenti tecnici, ma deriva, piuttosto, dalla contrapposizione fra rilievi modificativi e rilievi non modificativi degli elementi di prova. Spostando l'attenzione su quest'ultimo aspetto (la

---

[251] La possibilità di svolgere unilateralmente atti aventi valenza probatoria deve essere considerata come *extrema* ratio, quando risulti «improcrastinabile il suo compimento al fine della salvaguardia delle fonti di prova, suscettibili di repentina ed inevitabile dispersione o alterazione». Così, G. BELLANTONI, *Sequestro probatorio e processo penale*, Piacenza, 2005, p. 323.

[252] Cfr. *Nuovo codice di procedura penale*, a cura di G. CONSO – V. GREVI – G. NEPPI MODONA, IV, Padova, 1989, p. 829. In giurisprudenza, cfr. Cass., sez. II, 27 marzo 2008, Gori, in *CED Cass.*, n. 239774. In dottrina, v. D. CURTOTTI NAPPI, *I rilievi e gli accertamenti sul* locus commissi delicti *nelle evoluzioni del codice di procedura penale*, in D. CURTOTTI NAPPI – L. SARAVO (a cura di), *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze*, Torino, 2013, pp. 49 e 50.

potenziale modifica unilaterale della scena), è possibile apprezzare la seguente tesi: durante la fase di assicurazione delle fonti di prova (tracce, cose o luoghi pertinenti al reato), la polizia giudiziaria è legittimata a compiere tutte quelle attività che si rendano necessarie per garantire la conservazione della *scena criminis*, ad eccezione di quelle che sono di per sé lesive dell'obiettivo della preservazione della fonte originale. D'altronde, se i rilievi e gli accertamenti urgenti di cui all'art. 354, co. 2, c.p.p. hanno come obiettivo la conservazione delle prove, sarebbe contraddittorio e paradossale che fossero proprio questi la causa della alterazione dei reperti. Tutto ciò che è potenzialmente in grado di modificare la *scena criminis* originale necessita del contraddittorio con la controparte, da instaurarsi nelle forme dell'art. 360 o dell'art. 392 c.p.p., a seconda dell'urgenza della situazione concreta. Ragionare diversamente significherebbe ammettere l'esistenza di una irragionevole disparità di trattamento tra polizia giudiziaria, da un lato, e pubblico ministero e difensore, dall'altro, giacché in una simile situazione di urgenza alla prima sarebbe consentito di agire sacrificando la genuinità mentre ai secondi ciò sarebbe precluso. E' ovvio che non è così: anche se sollecitata dall'urgenza del provvedere, la modifica delle fonti di prova, per tradursi in un atto avente valenza probatoria deve essere sempre svolta in contraddittorio; l'intervento unilaterale urgente intanto può dar luogo a risultati probatori utilizzabili, in quanto dia garanzia di inalterabilità dell'originale.

In conclusione, le regole di utilizzabilità sono le stesse sia per i rilievi che per gli accertamenti tecnici: la ripetibilità dell'atto consente l'intervento unilaterale; la non ripetibilità impone il ricorso alla bilateralità, con il coinvolgimento della controparte in occasione del compimento di un'attività unica e finalizzata alla formazione della prova.

A ben guardare, quindi, i due istituti –rilievi e accertamenti tecnici- si influenzano a vicenda, integrando una disciplina valevole per tutti gli atti di indagine di natura tecnica, a prescindere dal nome e dal soggetto che li ponga in essere.

In particolare: 1) gli accertamenti tecnici attingono dai rilievi l'obbligo di conformità al protocollo desumibile *ex* art. 354, co. 2, c.p.p.; 2) i rilievi traggono dagli accertamenti tecnici il divieto di modificare unilateralmente la prova in assenza di contraddittorio, *ex* artt. 360 c.p.p. e 117 disp. att. c.p.p.

Quanto al primo aspetto, laddove in relazione alle particolarità delle circostanze concrete all'estrazione della copia forense provveda il pubblico ministero, *ex* artt. 359 c.p.p., o il difensore privato, a norma dell'art. 391-sexies c.p.p., la diversa qualificazione giuridica dell'attività (da rilievo ad accertamento tecnico) non affrancherebbe le parti dal dovere di

garantire conservazione ed integrità di quanto acquisito. Quindi, in ambito digitale, sia che si accerti, sia che si rilevi, il minimo comun denominatore è sempre il rispetto del protocollo, quale garanzia di conservazione e immodificabilità del dato.

Quanto al secondo aspetto, appare opportuno differenziare, all'interno della vasta categoria dei rilievi, quelli modificativi da quelli non modificativi della prova: questi ultimi possono senz'altro essere svolti unilateralmente in sede di sopralluogo, così come in occasione del compimento di atti a sorpresa, da ciascun soggetto e ciascuna parte in base alle rispettive attribuzioni e competenze; i rilievi modificativi, invece, sottostanno alla disciplina desumibile dal combinato disposto degli artt. 360 c.p.p. e 117 disp. att. c.p.p., senza alcuna eccezione. Ciò significa che è vietato ad una parte -sia che rilevi, sia che accerti- modificare unilateralmente l'elemento di prova senza instaurare il previo contraddittorio con la controparte.

4.3 Verso una disciplina giuridica unitaria del potere tecnico-investigativo

Nella fase delle indagini preliminari, le parole chiave che consentono di individuare la disciplina giuridica applicabile al c.d. "potere tecnico" delle parti e dei soggetti processuali sono due, "urgenza" e "alterabilità": urgenza significa indifferibilità dell'accertamento; alterabilità significa potenziale modificabilità dell'elemento di prova come conseguenza diretta e inevitabile dell'accertamento stesso[253].

Ebbene, le possibili combinazioni di questi due elementi sono quattro: 1) se l'attività di copia non comporta alcuna alterazione, neppure minima, del dato digitale e sussiste l'urgenza (*rectius,* indifferibilità), allora il suo svolgimento rientra a pieno titolo tra i rilievi esperibili a norma dell'art. 354, co. 2, c.p.p., ed il contraddittorio potrà essere solo eventuale; 2) se la copia, pur indifferibile, mette a rischio l'integrità dell'elemento di prova, l'equilibrio tra urgenza e diritto di difesa impone il ricorso alla procedura di cui all'art. 360 c.p.p., anticipando il contraddittorio, seppur debole, con la controparte; 3) in mancanza sia di urgenza che di potenziale alterabilità del dato, il potere tecnico delle parti è disciplinato dagli

[253] Tale distinzione emerge chiaramente *ex* artt. 360 c.p.p. e 117 disp. att. c.p.p., laddove si precisa che la non ripetibilità dell'accertamento tecnico può dipendere dal suo oggetto («persone, cose o luoghi il cui stato è soggetto a modificazione») o dalle modalità del suo svolgimento (quando «l'accertamento tecnico determina modificazioni delle cose, dei luoghi o delle persone tali da rendere l'atto non ripetibile»). Su tale aspetto, fra gli altri, cfr. O. BRUNO, *Un passo avanti: il confronto delle impronte digitali postula il rigore dell'art. 360 c.p.p. se il reperto va incontro a deterioramento o cancellazione*, in *Proc. pen. giust.*, 2013, p. 58.

artt. 348, co. 4[254], 359[255] e 391-sexies c.p.p.[256], a seconda che ad operare sia, rispettivamente, la polizia giudiziaria, il pubblico ministero o la difesa ed il contraddittorio torna ad essere solo eventuale; 4) in ipotesi di potenziale alterazione dell'elemento di prova e in assenza di urgenza, la sede privilegiata per l'espletamento dell'attività tecnica dovrebbe essere l'incidente probatorio, *ex* art. 392 c.p.p., il quale consente alle parti di esercitare, in condizioni di perfetta parità, quel contraddittorio forte finalizzato alla formazione della prova che dovrebbe essere la regola in un sistema processuale orientato in senso accusatorio. Le diverse garanzie partecipative[257], seppur in modo diverso a seconda delle circostanze, mirano a garantire il diritto al contraddittorio tecnico sulla prova, costituzionalmente inalienabile.

Tale approdo ermeneutico suscita istintivamente una immediata critica: come è possibile conciliare la disciplina degli artt. 360 c.p.p. e 117 disp. att. c.p.p. con l'urgenza che caratterizza gli atti esperibili *ex* art. 354, co. 2, c.p.p.? Nelle situazioni descritte da quest'ultima disposizione, infatti, il preavviso alla controparte potrebbe essere difficile se non addirittura impossibile da realizzare: la difficoltà si ravvisa in tutte le ipotesi in cui il sequestro rappresenta lo sbocco naturale di un precedente e preliminare atto a sorpresa (tipicamente, una perquisizione), incompatibile con qualsiasi tipo di preavviso; l'impossibilità si riscontra in tutti i casi in cui, in sede di sopralluogo, non esiste ancora nessun soggetto iscritto nel registro degli indagati da avvisare in funzione di garanzia.

---

[254] L'art. 348 c.p.p. (assicurazione delle fonti di prova) prevede espressamente la facoltà della polizia giudiziaria di compiere (di iniziativa o su delega del p.m.) atti o operazioni che richiedono specifiche competenze tecniche, avvalendosi dell'ausilio di persone idonee, il tutto al fine di assicurare le fonti di prova, cioè raccogliere ogni elemento utile alla ricostruzione del fatto ed alla individuazione del colpevole, ricercare le cose e le tracce pertinenti al reato nonché provvedere alla conservazione dello stato delle cose e dei luoghi. Più in dettaglio, il successivo art. 349 (identificazione della persona nei cui confronti vengono svolte le indagini e di altre persone) consente alla polizia giudiziaria di eseguire rilievi dattiloscopici, fotografici e antropometrici, nonché altri accertamenti" al fine di identificare l'indagato.

[255] A norma dell'art. 359 (consulenti tecnici del pubblico ministero) il p.m. ha la facoltà di avvalersi di esperti al fine di procedere ad «accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica».

[256] «1. Quando effettuano un accesso per prendere visione dello stato dei luoghi e delle cose ovvero per procedere alla loro descrizione o per eseguire rilievi tecnici, grafici, planimetrici, fotografici o audiovisivi, il difensore, il sostituto e gli ausiliari indicati nell'articolo 391-*bis* possono redigere un verbale nel quale sono riportati: a) la data ed il luogo dell'accesso; b) le proprie generalità e quelle delle persone intervenute; c) la descrizione dello stato dei luoghi e delle cose; d) l'indicazione degli eventuali rilievi tecnici, grafici, planimetrici, fotografici o audiovisivi eseguiti, che fanno parte integrante dell'atto e sono allegati al medesimo. Il verbale è sottoscritto dalle persone intervenute».

[257] Si va dal massimo delle garanzie in incidente probatorio (contraddittorio anticipato e forte) al minimo insopprimibile in sede di espletamento di atti a sorpresa (contraddittorio debole posticipato ed eventuale), passando dallo stadio intermedio rappresentato dai c.d. atti garantiti (i quali prevedono un contraddittorio sì debole, ma anticipato).

Ebbene, la soluzione a tale apparente *empasse* deriva da una corretta interpretazione del termine «necessari» di cui all'art. 354, co. 2, c.p.p. Dal latino *necessarius* che deriva da *ne* e da *cedĕre*, l'aggettivo "necessario" qualifica qualcosa "da cui non c'è modo di ritirarsi". Quindi, relativamente agli accertamenti e ai rilievi, indica atti dei quali non si può fare assolutamente a meno. L'urgenza *ex* art. 354, co. 2, dunque, si qualifica in base alla indifferibilità dell'atto, il quale non può che essere svolto nell'immediatezza dei fatti, pena l'impossibilità del suo successivo svolgimento. Facendo leva sul concetto di indifferibilità è possibile distinguere i rilievi veramente urgenti da quelli che appaiono solamente tali, ma che in realtà urgenti non sono, almeno secondo la logica dell'art. 354, co. 2, c.p.p.

Indifferibilità e irripetibilità, quindi, sono concetti diversi da tenere ben distinti: nel corso del sopralluogo, la polizia giudiziaria è legittimata a svolgere rilievi non ripetibili solo se essi sono al tempo stesso urgenti, ossia indifferibili («rilievi ora "o" mai più»[258]); quando, invece, esiste la possibilità del differimento, la mera non ripetibilità dell'atto («rilievi ora "e" mai più»[259]) non ne giustifica il compimento in maniera unilaterale. In altre parole, «gli unici rilievi irripetibili che la polizia giudiziaria può porre in essere sono quelli la cui irripetibilità discende dall'impossibilità […] di compiere il rilievo in un secondo momento», rimanendo esclusi, viceversa, quelli la cui non ripetibilità dipenda esclusivamente dal loro stesso compimento[260].

Con una precisazione: anche il rilievo non ripetibile e urgente, perché indifferibile, dovrebbe essere svolto in modo tale da preservare gli elementi di prova originali. Nell'ambito delle operazioni tecniche unilaterali non ripetibili, quindi, è necessario distinguere tra accertamenti modificativi della fonte di prova e accertamenti modificativi degli elementi di prova, ammettendo i primi ed evitando i secondi. In ogni caso, qualsiasi inevitabile modifica deve essere documentata e controllabile a posteriori. La controllabilità rappresenta il recupero, sul piano processuale, del *vulnus* determinato dall'inevitabile intervento unilaterale. Nel processo penale, infatti, non dovrebbe interessare la prova ad ogni costo: il fine non giustifica i mezzi, ma sono i mezzi, ossia il metodo e la procedura, a legittimare il fine.

---

[258] Così, A. CHELO, *Le prime indagini sulla scena del crimine*, cit., pp. 68 e 69.
[259] *Ibidem.*
[260] *Ibidem.*

5. La ripartizione dell'onere della prova digitale

L'art. 27, co. 2, Cost. introduce nel nostro sistema processuale una presunzione, seppur relativa, di innocenza[261] a favore del soggetto imputato. Come noto, in un'unica formula convivono una regola di trattamento ed una regola probatoria: la prima impone che l'imputato non sia assimilabile al colpevole se non dopo una condanna definitiva, il che si traduce nel divieto di anticipazione della pena; la seconda, letta in combinato disposto con l'art. 2728, co. 1, c.c.[262], prescrive che nel processo penale l'onere della prova circa la reità dell'imputato grava sulla parte che accusa. La parte su cui grava tale onere deve convincere il giudice della esistenza del fatto storico affermato attraverso gli elementi di prova acquisiti[263]. Va da sé che la parte su cui incombe l'onere della prova subisca poi, dal punto di vista processuale, le conseguenze svantaggiose derivanti dal non aver soddisfatto l'onere medesimo[264].

Nel processo penale, l'onere della prova grava quindi sul pubblico ministero, il quale deve dimostrare il fatto addebitato all'imputato, provandone la reità in modo da eliminare ogni ragionevole dubbio[265]. La difesa, invece, ha l'onere di provare la mancanza di credibilità delle fonti o l'inattendibilità delle prove raccolte dall'accusa, con la possibilità di fornire ricostruzioni alternative del fatto, in modo da insinuare un ragionevole dubbio sulla prospettazione offerta dall'accusa.

La mancata soddisfazione dell'onere della prova da parte dell'accusa ha come conseguenza, dal punto di vista processuale, l'assoluzione dell'imputato, *ex* art 530, co. 2, c.p.p.

In altre parole, dalla presunzione, seppur relativa, di innocenza dell'imputato, si ricava che è onere della parte che accusa acquisire fonti di prova genuine da cui estrapolare elementi di

---

[261] La dottrina tradizionale utilizza comunemente l'espressione "presunzione di non colpevolezza", che ha una palese connotazione negativa. Parla, più correttamente, di "presunzione di innocenza" P. TONINI, in C. CONTI – P. TONINI, *Il diritto delle prove penali*, cit., p. 69, interpretando - secondo l'insegnamento della Corte costituzionale, sentenze gemelle n. 348 e 349 del 2007 - la ambigua formula di cui all'art. 27, co. 2, Cost., alla luce dell'art. 6, co. 2, della Convenzione europea dei diritti dell'uomo, secondo cui «ogni persona accusata di un reato è presunta innocente sino a quando la sua colpevolezza non sia stata legalmente accertata».

[262] «Le presunzioni legali dispensano da qualunque prova coloro a favore dei quali esse sono stabilite».

[263] *Ex* art. 2697, co. 1, infatti, «chi vuol far valere un diritto in giudizio deve provare i fatti che ne costituiscono i fondamento».

[264] L'onere è definibile come la situazione giuridica attraverso la quale l'ordinamento impone ad un soggetto di comportarsi in un determinato modo, se questi vuole ottenere un qualche vantaggio.

[265] *Ex* art. 533, co. 1, c.p.p., così come modificato, nel 2006, con la legge n. 46. Ragionevole significa "comprensibile" da una persona razionale e "oggettivabile" in motivazione da parte del giudice attraverso gli elementi a disposizione. Cfr. C. CONTI, *Al di là di ogni ragionevole dubbio*, in AA.VV., *Novità su impugnazioni penali e regole di giudizio. La legge 20 febbraio 2006, n. 46*, coordinato da A. SCALFATI, Milano, 2006, pp. 102 e ss.

prova attendibili, mentre la difesa può limitarsi a dimostrarne esclusivamente il *deficit* di attendibilità per ottenere il vantaggio processuale connesso a siffatta ripartizione dell'onere della prova.

Il nodo interpretativo da sciogliere, quindi, consiste proprio nel comprendere fino a che punto si debba spingere la difesa per dimostrare la mancanza di attendibilità delle prove offerte dall'accusa.

In particolare, è legittimo chiedersi se a fronte della violazione delle *best practices* da parte degli inquirenti la difesa abbia l'onere di provare l'avvenuta manipolazione dei *files* introducendo elementi concreti da cui desumere il tipo di alterazione o possa limitarsi ad allegare il mancato rispetto del protocollo. Se la regola probatoria fosse la stessa del processo civile[266], la risposta sarebbe scontata: è onere della difesa provare il tipo di manipolazione lamentata. Senonché, nel processo penale esiste la regola probatoria della presunzione di innocenza che, letta insieme alla regola di giudizio del ragionevole dubbio, impone alla difesa un onere molto meno gravoso. Il ragionevole dubbio circa l'attendibilità della prova offerta dall'accusa ben si pone allegando esclusivamente il mancato rispetto di quel protocollo che la legge impone proprio a garanzia della genuinità della prova di natura digitale.

Ragionando diversamente, si imporrebbe alla difesa un onere della prova che non solo non le compete *ex* art. 27, co. 2, Cost., «ponendosi al di fuori dell'architettura sistematica del nostro ordinamento processuale[267]», ma che rasenta la c.d. "prova diabolica", non essendo possibile individuare *ex post* il tipo di alterazione subita dal *file*. Una simile prova sarebbe possibile, da parte della difesa, solo attivando quel contraddittorio anticipato *ex* art. 360 c.p.p., che, tuttavia, in sede di indagini informatiche non sempre è praticabile[268]. Il controllo successivo del verbale, *ex* art. 366, co. 1, c.p.p. e l'assistenza del difensore senza preavviso, *ex* art. 356 c.p.p., non consentono, infatti, di verificare e dimostrare tesi alternative, ma solo di sollevare eventuali difformità tra l'operato dell'autorità inquirente ed il protocollo desumibile *ex lege*.

Ed allora, il rispetto della procedura rappresenta l'unica ma fondamentale garanzia della corretta acquisizione della prova informatica nel processo penale, con la conseguenza che è

---

[266] *Ex* art. 2697, co. 2, c.c., infatti, «chi eccepisce l'inefficacia [dei fatti costitutivi del diritto] ovvero eccepisce che il diritto si è modificato o estinto, deve provare i fatti su cui l'eccezione si fonda». Medesimo standard probatorio, dunque, tra attore e convenuto, in ragione del fatto che nel processo civile i diritti sui quali si controverte si equivalgono.

[267] Così, A. E. RICCI, *Digital evidence e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc*., 2010, 3, p. 337.

[268] Non lo è, come detto, in caso di urgenza.

onere dell'accusa osservare il protocollo così come è onere della difesa contestarne la corretta applicazione; ma nulla di più[269].

6. Violazione dei protocolli e conseguenze processuali

Come abbiamo visto, il corretto "trattamento" dell'evidenza digitale costituisce un valore assoluto e non declinabile da parte dell'investigatore, qualunque sia l'attività tecnica posta in essere e chiunque sia il soggetto operante: non esistendo, «ad oggi, uno standard prestabilito per la metodologia di trattamento ed analisi delle prove informatiche […] l'unico principio cogente è quello relativo al mantenimento della integrità e non alterazione delle tracce fisiche dei dati informatici, i quali devono essere acquisiti al processo ed analizzati attraverso la copia degli stessi ottenuta tramite una procedura che ne assicuri la conformità»[270]. Nel precisare l'obiettivo finalistico della preservazione dei dati digitali da acquisire, la novella normativa non prende posizione dal punto di vista tecnico, giacché la stessa «allude a misure tecniche idonee, senza precisi riferimenti di disciplina. Ne consegue che trovano cittadinanza nel sistema di acquisizione della prova digitale le migliori pratiche delineate dalla prassi investigativa, dallo stato della tecnica e dagli operatori qualificati […] La prova digitale si accosta in tal modo alla prova scientifica»[271].

Ma quali sono, allora, le conseguenze processuali connesse alla violazione delle *leges artis*? Qual è l'effetto sul materiale probatorio della violazione o, peggio, dell'omissione delle *best practices* in occasione di attività, anche urgenti, di ricerca e acquisizione della prova digitale? La domanda è più che legittima, poiché, nonostante il silenzio del legislatore su tale

---

[269] «All'imputato spetta soltanto di mostrare che le modalità utilizzate per l'apprensione, per il mantenimento della *chain of custody* e per la successiva elaborazione non rispecchiano i canoni generalmente riconosciuti come affidabili. Ove ciò si appalesi, grava sull'accusa il peso di dimostrare che quel metodo, seppur difforme dalla migliore prassi tecnica, non ha, nel caso di specie, alterato i dati e ha salvaguardato la cosiddetta "integrità digitale". E in caso di incertezza su quest'ultima circostanza, si dovrà accogliere la regola di giudizio dell'*in dubio pro reo*, e non certo quella secondo cui *in dubio pro republica*». Così, L. LUPARIA, *Il caso Vierika: un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali*, in *Dir. int.*, 2006, p. 158. Nella giurisprudenza di merito, a favore di tale assunto cfr., oltre alla sentenza oggetto del presente commento, Tribunale di Chieti, 2 marzo 2006, in *Dir. dell'internet*, 2006, p. 572. Contra, Tribunale di Bologna, Sez. I, 22 dicembre 2005, in *Diritto dell'internet*, 2006, p. 153, dove si legge che «dal compimento di investigazioni informatiche che si discostano dalla migliore pratica scientifica non discende un'automatica inutilizzabilità del materiale probatorio raccolto. Spetta infatti alla difesa l'onere di dimostrare in che modo la metodologia utilizzata ha concretamente alterato i dati ottenuti».

[270] Così, Cass. pen., sez. feriale, 6 settembre 2012, Franchini, n. 44851, in

[271] Così, G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici,* cit., p. 189, il quale parla a tal proposito di «norme processuali in bianco».

punto, è chiaro a tutti che, ove tali prescrizioni non fossero presidiate da conseguenze processuali pregnanti, disquisire in ordine alla loro rilevanza sarebbe del tutto inutile.

La risposta a tale interrogativo è tutt'altro che semplice, perché si tratta di valutare le conseguenze, sul piano processuale, della violazione di regole tecniche non inserite nel codice di rito[272] e non standardizzate in ambito scientifico nazionale e internazionale[273]:

Ebbene, sul tema delle conseguenze processuali dell'inosservanza delle *best practices* in tema di trattamento di prove digitali dottrina e giurisprudenza si dividono. Da un lato, vi è chi sostiene che la risposta sanzionatoria andrebbe ricercata nell'ambito delle cause di invalidità degli atti: fra questi, esiste una ulteriore divisione tra coloro che sostengono l'ipotesi della nullità e coloro che invece militano a favore dell'inutilizzabilità degli atti. Dall'altro lato, più numerosi, si schierano coloro i quali parlano di mera irregolarità, riportando la questione nell'ambito della attendibilità/inattendibilità del materiale probatorio e ritenendo invocabile, come soluzione, il libero convincimento del giudice, opportunamente motivato.

6.1 Sulla irregolarità

In base ad un primo orientamento, di matrice giurisprudenziale[274], la (provata) violazione del protocollo di assicurazione, acquisizione e conservazione di dati informatici dovrebbe comportare esclusivamente l'inattendibilità del risultato ottenuto. In altre parole, la violazione o l'omissione delle c.d. *best practices* dovrebbe avere, come conseguenza processuale di tipo sanzionatorio, un atteggiamento di diffidenza del giudice rispetto al materiale non correttamente raccolto, secondo una presunzione di inadeguatezza che dovrebbe portare ad una valutazione giudiziale di inattendibilità probatoria.

A sostegno di tale tesi si invoca il principio di tassatività che pervade la materia delle cause di invalidità degli atti e che non consente di ricorrere all'inutilizzabilità (ma nemmeno alla nullità) per precludere all'evidenza digitale "mal trattata" l'accesso al materiale comunque legittimamente conoscibile da parte del giudicante: «la sanzione di inutilizzabilità è tassativa e

---

[272] Ma da questo solamente sottointese attraverso il riferimento a misure tecniche, prescrizioni e procedure in grado di assicurare conservazione e genuinità dei dati digitali.

[273] Numerose sono le raccolte di linee guida per l'approccio con la c.d. *scena criminis digitale*. Cfr., per un elenco delle migliori pratiche, L. LUPARIA – G. ZICCARDI, *Investigazione penale e tecnologia informatica*, cit. pp. 89-124.

[274] Con specifico riferimento alla materia della prova informatica, cfr.: Cass., sez. I, 26 febbraio 2009, Ammutinato, in C.E.D. Cass., n. 243922; Cass., sez. I, 25 febbraio 2009, n. 11503, Dell'Aversano, in C.E.D. Cass., n. 243495; Cass., sez. un., 21 aprile 2010, Mills, in C.E.D. Cass., n. 246584.

non può, pertanto, essere ampliata fino a ricomprendere l'inosservanza di regole scientifiche che non siano state recepite da una specifica normativa»[275]. Coerentemente con tale assunto, la mancata adozione di protocolli adeguati alle circostanze del caso concreto, la cui dimostrazione è il frutto di un accertamento di fatto insindacabile in sede di legittimità, inciderà, semmai, sulla valutazione giurisdizionale di credibilità della fonte e di attendibilità della rappresentazione, ma ciò presuppone la validità dell'elemento di prova e la sua utilizzabilità entro i binari del prudente apprezzamento del giudice, il quale, comunque, dovrà dare «conto nella motivazione dei risultati acquisiti e dei criteri adottati» (art. 192, co. 1, c.p.p). Seguendo questo ragionamento, la presunta violazione del protocollo rappresenta sempre e comunque una questione di fatto apprezzabile dal giudice di merito in base alle risultanze del caso concreto e risolvibile in base al principio del libero convincimento[276]. La garanzia per le parti rimane la congruità della motivazione, impugnabile in sede di appello. La conseguenza ultima, invece, è l'impossibilità di censurare tale aspetto in sede di legittimità.

D'altronde, si sostiene, «la legge si limita a porre un principio finalistico» senza «esplicita[re] le regole tecniche di acquisizione e di conservazione probatoria» e senza «diversifica[re] la qualità delle misure tecniche da adottare»[277], con la conseguenza che «l'idoneità a conservare e a non modificare il dato originale è giudizio tecnico rimesso in ultima analisi al prudente apprezzamento del giudice penale, che opera in qualità di *peritus peritorum*»[278].

A parere di coloro che sostengono tale orientamento, la tesi che fa leva sul libero convincimento del giudice è quella che maggiormente convince anche in ragione della *ratio* sottesa alla Convenzione di Budapest: realizzare le condizioni essenziali per assicurare un contrasto efficace ed effettivo al dilagare della criminalità informatica. Dal punto di vista processuale, questo obiettivo si è tradotto, da parte del legislatore della ratifica, nella

---

[275] Così, Cass., sez. II, 10 gennaio 2012, Dabellonio, in *CED Cass.*, n. 252796, in tema di rilievi dattiloscopici, asseritamente inutilizzabili perché eseguiti in difetto della documentazione fotografica dell'asportazione delle tracce dell'impronta, prevista dalla procedura codificata nei protocolli "standard".

[276] In dottrina, cfr. G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, cit., p. 190, secondo il quale «l'inosservanza delle misure tecniche idonee ad assicurare la salvaguardia della genuinità dei dati e delle informazioni raccolte si risolve sotto il profilo della valutazione della prova ed in particolare sul crinale della fondatezza dei risultati acquisiti. Se la raccolta delle prove informatiche non è stata conforme al modello legale, la circostanza riverbererà i suoi effetti sul valore e l'intensità della prova medesima, che sarà nondimeno utilizzabile ai fini della decisione, ma poco attendibile e dunque inidonea da sola a fondare un giudizio di colpevolezza secondo il prudente apprezzamento del giudice».

[277] Anzi, «viene sancita a priori l'indifferenza qualitativa fra le varie misure tecniche, tutte ab origine potenzialmente idonee ad assicurare il risultato probatorio». *Ivi*, p. 189.

[278] *Ivi*, p. 188.

previsione di strumenti di ricerca della prova in grado di migliorare l'approccio investigativo ed agevolare gli organi inquirenti «nell'accertare il tempo e il luogo dei commessi reati, aumentando la fruttuosità degli atti d'indagine e l'azione di contrasto alla criminalità informatica diffusa». Coerentemente con tale *ratio* di efficienza investigativa, «occorrerà […] evitare che le nuove norme divengano 'trappole della legittimità', evitando altresì di scorgere in ogni caso di difformità dal modello legale di acquisizione e conservazione della prova informatica un'ipotesi d'invalidità o di nullità dell'atto»[279].

6.2 Sulla nullità

Come noto, questa causa di invalidità colpisce l'atto del procedimento compiuto senza l'osservanza di quelle disposizioni che sono imposte dalla legge a pena di nullità. In materia vige uno stretto principio di tassatività, secondo il quale «l'inosservanza delle disposizioni stabilite per gli atti del procedimento è causa di nullità soltanto nei casi previsti dalla legge» (art. 177 c.p.p.). Sulla base del regime giuridico, le nullità si distinguono in assolute, intermedie e relative: sono colpite da nullità assoluta le inosservanze più gravi che sono previste dall'art. 179 c.p.p. e che riguardano i soggetti necessari del procedimento penale[280]; sono colpite da nullità a regime intermedio le inosservanze di media gravità previste nell'art. 180 c.p.p. e che riguardano una sfera più ampia di soggetti[281]; nullità relative, infine, sono quelle nullità speciali che non rientrano né tra quelle assolute, né tra quelle intermedie[282].

Ebbene, in base ad una lettura, di matrice dottrinale[283], la violazione delle *best practices* integrerebbe una ipotesi di nullità a regime intermedio, *ex* artt. 178, lett. c, e 180 c.p.p.

---

[279] *Ivi*, p. 186.

[280] Rientrano in questa categoria le violazioni delle disposizioni concernenti: «le condizioni di capacità del giudice» (intese nel senso di capacità generica all'esercizio della funzione giurisdizionale, come ad esempio la mancanza della laurea in giurisprudenza); «il numero dei giudici necessario per costituire i collegi» (salvo quanto previsto *ex* art. 33, co. 3, c.p.p.); «l'iniziativa del pubblico ministero nell'esercizio dell'azione penale». E' causa di nullità assoluta, inoltre, l'omessa citazione dell'imputato e l'assenza del difensore dell'imputato nei casi in cui ne è obbligatoria la presenza. Le ipotesi di nullità assoluta sono rilevabili anche d'ufficio in ogni stato e grado del procedimento e sono insanabili.

[281] Rientrano in questa categoria le violazioni delle disposizioni concernenti: la «partecipazione» del pubblico ministero al procedimento; «l'intervento, l'assistenza e la rappresentanza dell'imputato e delle altre parti private nonché la citazione in giudizio della persona offesa dal reato e del querelante». Le nullità intermedie sono rilevabili anche d'ufficio, ma entro determinati limiti di tempo, e sono sanabili.

[282] Ad esempio, l'art. 199, co. 2, c.p.p., che impone, a pena di nullità, che i prossimi congiunti dell'imputato siano avvisati della facoltà di astenersi dal deporre come testimoni. Le nullità relative sono dichiarabili dal giudice solo su eccezione della parte interessata entro limiti di tempo molto ristretti e sono sempre sanabili.

[283] Cfr. A. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. int.*, 2008, 5, p. 509.

Secondo tale orientamento, all'indomani della novella del 2008 l'adozione da parte degli investigatori di adeguate misure di preservazione della prova digitale rappresenterebbe uno speciale requisito, con finalità garantiste, delle fattispecie che a vario titolo si occupano di raccolta di informazioni di natura digitale[284]. In particolare, la corretta conservazione dei dati originali rappresenta il requisito indefettibile al fine di assicurare la ripetibilità dell'accertamento investigativo, a tutela del contraddittorio tecnico delle parti. Non garantire la conservazione, quindi, significa impedire alla controparte di «partecipare» alla formazione della prova, con conseguente nullità, a regime intermedio, del preliminare atto investigativo posto in essere unilateralmente in modo scorretto. In altre parole, la correttezza metodologica dell'accertamento rende quest'ultimo ripetibile, di conseguenza il suo espletamento non priva le altre parti interessate del diritto di confrontarsi con la prova rappresentativa di tipo reale. Viceversa, l'alterazione unilaterale della prova esige l'applicazione dell'art. 360 c.p.p., con tutte le garanzie difensive di tipo partecipativo in esso previste: la mancata adozione di tali prerogative viola le disposizioni concernenti «l'intervento, l'assistenza e la rappresentanza dell'imputato e delle altre parti private», con conseguente nullità dell'atto a norma del combinato disposto degli artt. 178, lett. c e 180 c.p.p.

6.3 Sulla inutilizzabilità

Seppur per motivi differenti, nessuna delle due tesi sopra esposte merita di essere condivisa, né quella che predica la nullità, né, tantomeno, quella che sostiene la mera irregolarità delle prove raccolte in violazione delle *best practices*. La prima non coglie nel segno poiché non tiene conto dell'esatta portata del principio di tassatività in tema di nullità. Da tale principio, infatti, deriva un vero e proprio divieto di analogia in tema di cause di invalidità degli atti. Quanto alla seconda tesi, l'equivalenza tra violazione del protocollo e inattendibilità del risultato non soddisfa fino in fondo le esigenze di garanzia delle parti coinvolte nell'accertamento.

In base ad un terzo, più rigoroso e corretto orientamento, la violazione del protocollo di acquisizione della prova digitale dovrebbe determinare, come conseguenza processuale, la

[284] In qualità di elemento costitutivo di tali fattispecie, la imperfetta o la mancata adozione di uno *stardard* adeguato impedirebbe a tali fattispecie di integrarsi. Cfr. G. CONSO, *Il concetto e le specie d'invalidità*, Milano, 1972, pp. 19 e ss.; P. MOSCARINI, *Art. 184 c.p.p.*, in AA.VV., *Commentario breve al codice di procedura penale*, a cura di G. CONSO E V. GREVI, Padova, 1987, pp. 611 e ss.

inutilizzabilità del materiale probatorio illegittimamente acquisito, *ex* art. 191, co. 1, c.p.p. A tale draconiana conclusione è possibile giungere percorrendo almeno due sentieri differenti: 1) quello della inutilizzabilità per violazione del dovere giudiziale di escludere, già in fase di ammissione della prova (art. 190 c.p.p.), l'evidenza digitale a causa della sua oggettiva inidoneità probatoria[285]; 2) quello della inutilizzabilità a causa della mancanza, in ipotesi di violazione/omissione del protocollo, del potere istruttorio in capo all'autorità inquirente[286].

6.3.1 Sulla inidoneità probatoria

A mente dell'art. 190 c.p.p., «le prove sono ammesse su richiesta di parte. Il giudice provvede senza ritardo con ordinanza escludendo le prove vietate dalla legge e quelle che manifestamente sono superflue o irrilevanti». Ebbene, a fronte di una prova scientifica, tipica o atipica che sia, il doveroso giudizio di rilevanza non può prescindere dalla valutazione dell'astratta idoneità probatoria dell'elemento/dato già in fase di ammissione. Tale criterio di idoneità probatoria è esplicitamente ribadito con riferimento alla prova atipica *ex* art. 189 c.p.p., laddove si richiede «l'idoneità ad assicurare l'accertamento dei fatti», ma «non può esservi dubbio che l'esistenza di questo presupposto sia implicito anche nel caso di prove tipiche»[287]. Con la seguente precisazione: nel caso di prove atipiche, l'idoneità va dimostrata in concreto e l'onere di tale dimostrazione grava sulla parte che ne richiede l'ammissione; nel caso di prove tipiche, l'idoneità è presunta, ma tale presunzione è solo relativa, al punto da poter essere smentita dalla scienza.

Ebbene, una prova scientifica priva di idoneità probatoria, perché fondata su criteri scientifici non attendibili, è inammissibile. Ma l'inammissibilità costituisce una regola di esclusione e non di valutazione della prova. Di conseguenza, si è affermato che

---

[285] Infatti, il criterio dell'idoneità probatoria, espressamente indicato dall'art. 189 c.p.p. ai fini dell'ammissione della prova atipica, è implicitamente riconosciuto come uno dei presupposti per l'ammissione anche della prova tipica, *ex* art. 190 c.p.p. In dottrina, cfr. BRUSCO, *La valutazione della prova scientifica*, in *Dir. pen. proc.*, 2008, suppl. al n. 6, p. 27.

[286] «Quando si tratta di forme essenziali, il mancato rispetto del modello legale [deve] essere equiparato ad una carenza di potere istruttorio che comporta inutilizzabilità. Un'interpretazione "sostanziale", basata sull'interesse protetto, parrebbe condurre a conclusioni del genere». Così, C. CONTI, *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali*, in *Cass. pen.*, 2013, vol. 53, fasc. 2, p. 485. V., *amplius*, C. CONTI, in P. TONINI – C. CONTI, *Il diritto delle prove penali*, cit., pp. 331 e ss. In giurisprudenza, a favore di quest'ultima interpretazione, cfr, Cass., sez. III, 22 aprile 2010, Fiorillo, in C.E.D. Cass., n. 246598. Contra, cfr.: Cass., sez. VI, 6 ottobre 2010, Drago, in C.E.D. Cass., n. 248527; Cass., sez. II, 1 gennaio 2012, Dabellonio, in C.E.D. Cass., n. 252796.

[287] Così, C. BRUSCO, *La valutazione della prova scientifica*, cit., p. 27.

«l'ammissione di una prova fondata su criteri scientifici non attendibili costituisce violazione di norma processuale [l'art. 190 c.p.p.] sia perché inidonea alla funzione probatoria sia perché irrilevante non potendo essere posta dal giudice a fondamento della sua decisione […] E se la prova è stata erroneamente ammessa, il giudice non la può utilizzare per la decisione trattandosi di prova acquisita in violazione di un divieto stabilito dalla legge (art. 191, co. 1, c.p.p.)»[288].

Senonché, il filtro giurisdizionale di ammissibilità della prova, per espressa previsione codicistica, è composto da maglie piuttosto larghe, dovendo il giudice escludere dal processo le sole prove «manifestamente» superflue o irrilevanti. Un giudizio difficile da realizzare «senza ritardo con ordinanza» (art. 190, co. 1, c.p.p.). La conclusione appare davvero scontata: «se l'affidabilità della prova è […] dubbia non credo sia possibile parlare di regola di esclusione; del resto ovvie ragioni di prudenza consiglierebbero, in questi casi, di ammetterla e di riservare alla fase della decisione la soluzione del problema»[289].

6.3.2 Sulla carenza di potere istruttorio

In base ad un'altra teoria, di matrice dottrinale[290] ma che ha trovato riscontro, seppur isolato, nella giurisprudenza di legittimità[291], è necessario distinguere tra forme essenziali e forme non essenziali degli atti, soprattutto quando questi si riferiscono a prove di natura scientifica.

Di regola, il mancato rispetto delle modalità di acquisizione di una prova è causa di inutilizzabilità solo se ciò è espressamente previsto come conseguenza esplicita di tale inosservanza modale: in tal caso si parla di inutilizzabilità speciale. Di inutilizzabilità generale, *ex* art. 191, co. 1, c.p.p. viceversa si può parlare solo con riferimento a violazioni che attengono all'*an*, e non al *quomodo*, ossia in presenza dell'esercizio di un potere istruttorio che in realtà non sussiste. Senonché, come ogni regola anche questa conosce delle eccezioni: «quando si tratta di forme "essenziali", il mancato rispetto del modello legale [deve] essere equiparato ad una carenza di potere istruttorio che comporta inutilizzabilità.

---

[288] *Ibidem*. V, inoltre, S. MAFFEI, *Ipnosi, poligrafo, narcoanalisi, risonanza magentica: metodi affidabili per la ricerca processuale della verità?*, in DE CATALDO NEUBERGER (a cura di), *La prova scientifica nel processo penale*, Padova, 2007, p. 417.

[289] Così, C. BRUSCO, *La valutazione della prova scientifica*, cit., p. 27.

[290] C. CONTI, in P. TONINI – C. CONTI, *Il diritto delle prove penali*, cit., pp. 331 e ss.

[291] Cass., sez. III, dep. 27 aprile 2010, Fiorillo, in *CED Cass.*, n. 246598, con riferimento, nel caso concreto, ad un'attività di campionamento e di analisi di rifiuti.

Un'interpretazione 'sostanziale', basata sull'interesse protetto, parrebbe condurre a conclusioni del genere»[292].

Calata nel contesto digitale, tale teoria ha degli effetti dirompenti: ciascuna parte ha la possibilità di acquisire l'evidenza digitale esclusivamente rispettando l'imperativo codicistico della conservazione e della genunità di quanto appreso, con la conseguenza che la mancata osservanza di tecniche astrattamente in grado di garantire tale risultato dovrebbe comportare una carenza di potere istruttorio[293]. Agire comunque significherebbe violare un divieto nell'*an* che avrebbe, come conseguenza, l'inutilizzabilità di quanto acquisito *ex* art. 191, co. 1, c.p.p.

D'altronde, il giudice, in base al proprio "libero convincimento" (art. 192, comma 2, c.p.p.), potrebbe sì ritenere l'evidenza digitale mal raccolta priva di qualsiasi valenza dimostrativa in quanto inaffidabile[294], ma, invocando il medesimo principio, potrebbe ritenersi autorizzato ad affermare l'esatto contrario, valutando comunque come attendibile la prova ove corroborata da ulteriori elementi di conferma[295].

Ragionare in questi termini, a ben guardare, significa far rivivere, in ambito di prova informatica, la teoria della "convergenza del molteplice" [296], propria della prova critica o indiziaria. Tuttavia, a seguito della sentenza Franzese[297], tale orientamento non merita di essere condiviso, né con riferimento alla prova per indizi[298], né, tantomeno, con riferimento alla prova rappresentativa di tipo reale, dove, *a fortiori*, il deficit rappresentativo di ciascun elemento di prova non può essere colmato attraverso una co-valutazione globale degli altri elementi a disposizione[299].

---

[292] Così, C. CONTI, *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali*, cit., p. 493.

[293] Si tratta, volendo utilizzare una terminologia di matrice anglosassone, della inutilizzabilità per *unreliability*.

[294] Soluzione accolta, ad esempio, da Tribunale di Chieti, 2 marzo 2006, in *Dir. dell'internet*, 2006, p. 572, con nota di F. CAJANI, *Alla ricerca del log (perduto)*.

[295] Soluzione accolta da Tribunale di Bologna, 22 dicembre 2005, in Dir. dell'internet, 2006, p. 153, con nota critica di L. LUPARIA, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali*, cit., p. 152.

[296] In dottrina, cfr.: V. RUSSO – A. ABET, *La prova indiziaria e il "giusto processo". L'art. 192 c.p.p. e la legge 63/2001*, Napoli, 2001, p. 37; E. GIRONI, *La prova indiziaria*, in AA.VV., *La prova penale*, trattato diretto da A. GAITO, vol. III, Torino, 2008, pp. 139-141; C. ZAZA, *Il ragionevole dubbio nella logica della prova penale*, Milano, 2008, pp. 118 e ss. In giurisprudenza, v. Cass., sez. I, 5 marzo 1991, Calò, in Cass. pen., 1992, p. 1010.

[297] Cass., sez. un., 11 settembre 2002, Franzese, in *Guida dir.*, 2002, n. 38, p. 62.

[298] In dottrina, cfr.: P. TONINI – C. CONTI, *Il diritto delle prove penali*, cit., pp. 91-95; F. M. MOLINARI, *Dubbio sull'attendibilità della chiamata in correità ed attribuzione alla stessa di un valore indiziante*, in *Cass. pen.*, 1996, p. 1918; S. BATTAGLIO, *"Indizio" e "prova indiziaria" nel processo penale*, in *Riv. it. dir. proc. pen.*, 1995, p. 375; E.M. CATALANO, voce *Prova (canoni di valutazione della)*, in *Dig. disc. pen.*, agg. II, 2008, p. 794. In giurisprudenza, v. Cass., sez. I, 16 giugno 2008, Di Tella, in C.E.D. Cass., n. 216181.

[299] Concetto chiaro sin dal 1764, anno in cui Cesare Beccaria scriveva: «Quando le prove di un fatto sono dipendenti l'una dall'altra, cioè quando gl'indizi non si provano che fra di loro, quanto maggiori prove si adducono tanto è minore la probabilità del fatto, perché i casi che farebbero mancare le prove antecedenti fanno

Peraltro, «un simile ragionamento […] oltre a sovrapporre indebitamente due differenti fasi del procedimento probatorio (assunzione e valutazione), pare costituire il frutto di un'inversione metodologica, giacché il giudice è chiamato a valutare –sia pure con cautela- proprio ciò che la legge avrebbe voluto sottrarre a siffatto sindacato. Le regole poste a tutela dell'attendibilità servono proprio ad evitare che al giudice sia consegnato un elemento la cui idoneità accertativa non è "accreditata" *ex ante* dalla *lex probatoria*. Pertanto, confidare in un recupero della tutela al momento della valutazione significherebbe affidare la giudice un elemento il cui impiego avrebbe dovuto essergli per legge escluso. In tal modo, le regole di esclusione finiscono per snaturarsi tornando al meccanismo, di sapore inquisitorio, in base al quale il libero convincimento è un *passpartout* idoneo a superare qualsivoglia limite»[300].

In un campo spinoso e irto di insidie come quello tecnico-digitale, la "valvola di sfogo" del libero apprezzamento giurisdizionale rischia di vanificare lo sforzo del legislatore, svilendo l'importanza della riforma del 2008.

7. Le acquisizioni digitali all'estero ai sensi del nuovo art. 234-*bis* c.p.p.

La legge n. 43 del 2015, di conversione del d.l. n. 7 del 2015[301], ha introdotto nel codice di rito l'art. 234-*bis*, per effetto del quale «E' sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare».

Nonostante il nobilissimo fine del legislatore della novella[302], la norma appare avulsa dal sistema e foriera di non pochi dubbi interpretativi. In particolare, *prima facie* emergono

---

mancare le susseguenti. […] Quando le prove sono indipendenti l'una dall'altra, cioè quando gli indizi si provano d'altronde che da sé stess, quanto maggiori prove si adducono, tanto più cresce la probabilità del fatto, perché la fallacia di una prova non influisce sull'altra». C. BECCARIA, *Dei delitti e delle pene*, Livorno, 1764.

[300] Così, C. CONTI, *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali*, cit., pp. 485 e ss. V., amplius, C. CONTI, *Il volto attuale dell'inutilizzabilità: derive sostanzialistiche e bussola della legalità*, in *Dir. pen. proc.*, 2010, pp. 781-797.

[301] Recante «Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione».

[302] Nell'incipit del testo del decreto-legge si può leggere come «la straordinaria necessità ed urgenza, anche alla luce dei recenti gravissimi episodi verificatisi all'estero, di perfezionare gli strumenti di prevenzione e contrasto del terrorismo, anche attraverso la semplificazione delle modalità di trattamento di dati personali da parte delle Forse di polizia, nel rispetto dei diritti riconosciuti ai soggetti interessati dalle norme vigenti in materia; ... la straordinaria necessità e urgenza di adottare misure urgenti, anche di carattere sanzionatorio, al fine di prevenire

perplessità che, in concreto, si sostanziano in due quesiti, la cui risposta è lungi dall'essere di immediata percezione, sul chi debba intendersi per «legittimo titolare» dei documenti e dei dati informatici conservati all'estero e, soprattutto, se la norma in commento fornisca uno strumento che, nell'ottica del legislatore, sia in grado di sostituire altre forme di cooperazione giudiziaria o, addirittura, la procedura rogatoriale[303].

Quanto al primo interrogativo, se per legittimo titolare dei dati si intende il soggetto che li ha formati e che li detiene all'estero, allora la norma è priva di senso e ciò per due motivi fondamentali: a fronte di una eventuale richiesta, il rifiuto di consegnare i dati da parte di tale soggetto renderebbe la norma *inutiliter data*; inoltre, anche qualora vi fosse il consenso, la persona sospettata verrebbe a conoscenza dell'attività investigativa nei suoi confronti, con evidente nocumento per la prosecuzione delle indagini. Solo qualora si intenda per legittimo titolare il gestore dei dati, lo strumento potrà avere una qualche efficacia[304].

Quanto al secondo interrogativo, pare fuori luogo sostenere che il nuovo art. 234-*bis* c.p.p. sia in grado di derogare al vigente sistema rogatoriale: è da ritenere che si debba ricorrere alla rogatoria verso l'estero per ottenere la traslazione nel fascicolo processuale dei documenti e dei dati informatici in argomento. Qualora manchi un accordo bilaterale tra l'Italia e lo Stato detentore del documento o dei dati informatici, non pare che questa possa essere superata dalla norma in questione, la quale, avendo una valenza unilaterale, non potrà influire sulle determinazioni dello Stato richiesto della collaborazione internazionale. Nessuna deroga,

---

il reclutamento nelle organizzazioni terroristiche e il compimento di atti terroristici, rafforzando altresì l'attività del Sistema di informazione per la Sicurezza della Repubblica; ... la straordinaria necessità ed urgenza di introdurre disposizioni per assicurare il coordinamento dei procedimenti penali e di prevenzione in materia di terrorismo, anche internazionale...», rendesse necessario adottare una procedura che consentisse di rendere più efficace il contrasto al terrorismo di matrice internazionale.

[303] Per una esauriente trattazione degli strumenti "tradizionali" finalizzati alla raccolta transnazionale delle prove, cfr. M. DANIELE, *La cooperazione giudiziaria. Ricerca e formazione della prova*, R. E. KOSTORIS (a cura di), *Manuale di procedura penale europea*, Milano, 2014, pp. 301 e ss.

[304] Con la seguente precisazione: non potranno avere ingresso attraverso questa norma quegli atti che, sebbene provvisti del consenso all'utilizzo da parte del "legittimo titolare", siano comunque assimilabili, quanto al loro contenuto, ai documenti anonimi di cui all'art. 240 c.p.p. Altrettanto scontata è l'inammissibilità, come prova, di documenti provenienti da imprecisate fonti estere che in realtà contengono valutazioni, asserzioni, dichiarazioni che, nel nostro processo penale, devono necessariamente soggiacere al vaglio del contraddittorio. Sul punto è bene ricordare l'orientamento della Suprema Corte secondo cui «Il documento rappresentativo di un atto descrittivo o narrativo può fungere da prova soltanto qualora la dichiarazione documentata rilevi di per sé come fatto storico, e non esclusivamente come rappresentazione di un fatto, poiché in tale ultima ipotesi, essa va acquisita e documentata nelle forme del processo, risultando altrimenti violato il principio del contraddittorio». Cfr. Cass. pen., sezione II, 4 ottobre 2007, n. 38871, in *CED*, 2007, rv. 238220.

inoltre, sussiste al vigente sistema di cooperazione in ambito europeo e internazionale che già consente la rapida circolazione di prove documentali di questo genere[305].

Resta da considerare se le procedure di acquisizione di questo materiale debbano o meno osservare gli standard che nel nostro ordinamento sono fissati dagli art. 254-*bis* e 352, comma 1-*bis*, del codice di procedura penale per le acquisizioni informatiche, telematiche e di telecomunicazione, tra le quali figurano la garanzia di conservazione degli originali e quella di conformità a questi ultimi delle relative copie. A meno di non voler incorrere in una irragionevole disparità di trattamento dei soggetti che detengono i dati in server allocati sul territorio nazionale piuttosto che in siti all'estero, la risposta non può che essere affermativa: lo standard qualitativo del documento informatico non cambia a seconda del luogo ove questo è detenuto.

In conclusione, probabilmente l'unico modo per "salvare" il contenuto dell'art. 234-*bis* consiste nell'intendere tale norma come strumento finalizzato ad un'attività di prevenzione ai fini di un'efficace intelligence. Ma anche in questo senso, se la ratio del legislatore fosse stata davvero la prevenzione, intesa come ricerca di elementi utili ad azionare un eventuale procedimento penale, è opportuno chiedersi a cosa è dovuta l'infelice collocazione sistematica della norma tra i mezzi di prova.

Saranno, forse, le prime applicazioni pratiche a dipanare questi primi dubbi interpretativi che, tuttavia, dimostrano come spesso certi interventi siano adottati sulla scorta di impulsi più che giustificati, ma avulsi dal sistema in cui debbono operare.

---

[305] Cfr. M.F. CORTESI, *Il Decreto antiterrorismo. I riflessi sul sistema processuale, penitenziario e di prevenzione*, in *Dir. pen. proc.*, 2015, 8, p. 950.

PARTE SECONDA
INDAGINI INFORMATICHE OCCULTE:
LA PROVA DIGITALE *ON LINE*

CAPITOLO 3
IL CAPTATORE INFORMATICO

Sommario: 1. Il punto di vista tecnico-operativo – 2. Il punto di vista tecnico-giuridico – 2.1 Tipicità o atipicità? – 2.2 Sull'art. 189 c.p.p. – 2.3 Prova atipica o prova incostituzionale? - 2.3.1 Prova atipica e riserva di legge - 2.3.2 Prova atipica e riserva di giurisdizione – 2.3.3. Prova atipica in assenza di riserve – 3. Il bene giuridico in gioco - 4. Dal diritto alla prassi: prova atipica o prova irrituale? Il principio di non sostituibilità - 5. Virus di Stato e diritto vivente: i precedenti in Italia - 5.1 La sentenza "Virruso" – 5.2 Il caso "Bisignani" – 5.3 Il caso "Ryanair" - 6. Uno sguardo oltre i confini nazionali - 6.1 La Corte costituzionale tedesca - 6.2 Qualche timido tentativo legislativo - 7. Considerazioni conclusive - 7.1 *De iure condito* -7.2 *De iure condendo*.

1. Il punto di vista tecnico-operativo

Il "captatore informatico"[306] consiste in un *software*, o, più precisamente, in un *malware*[307] che, una volta installato (furtivamente) all'interno di un determinato sistema informatico obiettivo[308], consente ad un centro remoto di comando di prenderne il controllo, sia in termini di *download* che in termini di *upload* di dati e informazioni di natura digitale. Il *software* è costituito da due moduli principali, un programma *server* ed un programma *client*: il *server* è

[306] Su questo nuovo strumento di indagine, vedi S. MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, cit., pp. 2855 e ss.; ID, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, In *Cass. pen.*, 2015, n. 2. Cfr., inoltre, S. ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del cloud criminal*, cit., pp. 1 e ss.; S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. Pen.*, 1, 2014; M. TROGU, *Sorveglianza e "perquisizioni" on-line su materiale informatico*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, p. 431; E. APRILE, voce *Captazioni atipiche (voci, immagini, segnali)*, in A. SCALFATI (diretto da), *Dig. proc. pen. on line*, Torino, 2012. Per una analisi comparata: con specifico riferimento all'esperienza tedesca, cfr. R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online* durchsuchung, cit., pp. 679 e ss.; quanto all'esperienza statunitense, v. F. CERQUA, *Le investigazioni informatiche e la protezione dei dati personali negli Stati Uniti ed in Italia: due modelli a confronto*, cit., pp. 775 e ss.

[307] In ambito di sicurezza informatica, il termine *malware* indica genericamente un qualsiasi *software* creato con il solo scopo di causare danni più o meno gravi ad un computer, ai dati degli utenti del computer, o ad un sistema informatico su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* ed ha dunque il significato letterale di "programma malvagio". *Malware*, in realtà, è concetto di genere che comprende tutte le diverse *species* di *virus* conosciuti: *virus* in senso stretto (*virus* di file, *virus* di *boot*, *virus* multipartiti e *virus* di macro), *worms*, *trojan* e *backdoors*. Da un punto di vista informatico, un *virus* non è altro che un programma che si attiva e comincia a diffondersi in modo totalmente indipendente dalla volontà dell'utente. I virus non sono capaci di un comportamento autonomo: tutto ciò che sono in grado di fare è stato puntualmente previsto (come un qualsiasi programma per computer) dai programmatori che li hanno ideati e scritti.

[308] Sia esso un personal computer, fisso o portatile, sia esso un *tablet* o uno *smarthpone* di ultima generazione.

il programma di piccole dimensioni che infetta il dispositivo "bersaglio"; il *client*, invece, è l'applicativo che il "pirata" usa per controllare il dispositivo infetto.

I programmi spia possono essere inseriti nel sistema informatico "bersaglio" sia da remoto, sia da vicino. Nel primo caso il collegamento tra client e server viene realizzato a distanza, attraverso l'invio, tramite la rete Internet, di un c.d. *virus trojan*, cioè un programma ambiguo, dalla doppia faccia, costituito da una componente nota all'utente, il quale installa il programma proprio per ottenerne le funzionalità a lui familiari (il cavallo di Troia, appunto), e una componente non nota, rappresentata da quella parte del programma che cela un codice segreto in grado di creare un collegamento occulto tra il dispositivo su cui è installato il server ed il computer remoto di controllo. Tale collegamento, che consente di fatto all'utente del computer remoto di avere il pieno controllo del sistema informatico "bersaglio", viene creato inconsapevolmente dall'utente di quest'ultimo attraverso l'installazione del programma nella sua componente nota e palese.

Nel secondo caso, il collegamento tra client e server viene realizzato intervenendo fisicamente a livello hardware sul dispositivo da controllare: l'intervento tecnico, in questo caso, consiste nell'inserimento, da parte del controllore, di una *backdoor* all'interno del dispositivo "bersaglio" in maniera del tutto simile a quanto avviene per l'installazione di una microspia finalizzata ad una intercettazione ambientale.

La "riuscita" del monitoraggio in termini investigativi dipende, evidentemente, dall'ignara "collaborazione" dell'utente del sistema "bersaglio", che deve, nel caso di aggressione di tipo software, installare sul proprio dispositivo il file di sistema mascherato, per ipotesi, da software di aggiornamento, o, in caso di aggressione hardware, lasciare incustodito l'apparecchio il tempo necessario, dal punto di vista tecnico, per l'intervento fisico da parte dell'operatore di polizia giudiziaria o del suo ausiliario. Evidentemente, non sempre è possibile fare affidamento su tale ignara collaborazione, soprattutto quando gli inquirenti hanno a che fare con soggetti inseriti in contesti criminali di un certo livello, abituati a diffidare di *input* provenienti da fonti sconosciute e spesso assistiti da consulenti estremamente competenti in materia di sicurezza informatica. In questi casi, l'unica alternativa per ottenere il controllo da remoto del dispositivo *target* consisterebbe nell'affidarsi alla collaborazione del gestore del flusso informativo del sistema informatico

attenzionato, esattamente come avviene in ipotesi di intercettazione telematica[309]. Ci si riferisce, in particolare, alla necessità che, dietro compenso, il gestore fornisca all'autorità giudiziaria una linea dati in cui far confluire le informazioni digitali che vedono coinvolto, come mittente o come destinatario, il sistema informatico/telematico bersaglio. Ma ciò rappresenta una ipotesi certo auspicabile, ma appartenente ad un futuro ancora troppo lontano dalla realtà quotidiana della prassi operativa.

Quando si discute di controllo remoto di dispositivi digitali è sempre opportuno riferirsi al plurale e mai al singolare: non esiste, infatti, un unico *software*, ma diversi programmi tecnicamente in grado di intaccare la sicurezza dei dati e delle informazioni dei dispositivi bersaglio. Tali programmi, peraltro, lungi dall'avere una lunga vita operativa, sono destinati all'obsolescenza precoce, dovendosi adeguare in tempo reale al continuo sviluppo della tecnologia difensiva (antivirus) in grado di bloccare sul nascere i tentativi di infiltrazione dei *virus*, anche di quelli di Stato. In altre parole, il "captatore informatico" è concetto di genere, all'interno del quale è possibile individuare *species* molto diverse dal punto di vista tecnico-informatico.

Ai nostri fini, tuttavia, appare di fondamentale importanza la *summa divisio* tra *online search* e *online surveillance*. I programmi spia appartenenti alla prima categoria consentono di far copia, totale o parziale, delle unità di memoria del sistema informatico "attenzionato". In particolare, tale tipologia di software è tecnicamente in grado di entrare in maniera occulta all'interno del dispositivo "bersaglio" al fine di estrapolare dati e informazioni che, una volta "copiati", vengono trasmessi, in tempo reale o ad intervalli prestabiliti, agli organi di

[309] Come noto, le intercettazioni telefoniche tradizionali vengono effettuate intercettando la comunicazione direttamente sui server dell'azienda telefonica. Su uno di questi server, appositamente attrezzato per questo scopo, il traffico telefonico viene diviso in due flussi. Il primo prosegue la sua strada "naturale" giungendo a destinazione. Il secondo viene "copiato" su un disco fisso ed analizzato. Questa tecnica è esattamente la stessa sia nel caso dei telefoni fissi che di quelli mobili. In questo caso, non ci sono né ritardi nella consegna dei pacchetti e né tracce digitali od analogiche che possano far pensare ad un'intercettazione in corso. In particolare, le intercettazioni si realizzano principalmente attraverso una linea definita Res, che può essere presa a noleggio dalla Procura presso il gestore telefonico, oppure presso società private o consorzi che dispongono di un certo numero di queste linee. La linea telefonica Res collega la rete telefonica cui fa capo l'utenza (rete mobile Tim, oppure rete di telefonia fissa Telecom) alla sala intercettazioni della Procura, dove vi è un server presso il quale viene convogliato tutto il traffico telefonico di quella utenza o delle utenze di cui l'autorità giudiziaria ha disposto le intercettazioni. Si utilizzano veri e propri computer che hanno la capacità di memorizzare non solo la parte fonica, ma anche tutta la trasmissione dati, e di gestire agevolmente l'attività di intercettazione. Queste apparecchiature possono trovarsi presso la Procura, ma spesso vengono "remotizzate", cioè l'intercettazione arriva in Procura ma il segnale viene fatto rimbalzare presso gli uffici della polizia giudiziaria. Al termine del periodo autorizzato dalla magistratura, il gestore della linea Res, del server e di questa macchina, che è sempre un privato, effettua uno scarico dei dati contenuti nella macchina e li copia su un supporto magnetico, che normalmente è un cd o un dvd. A quel punto il cd può essere ascoltato dal magistrato e può essere trascritto da un perito o consulente. Quando una traccia è stata memorizzata su un cd o dvd non è modificabile, può essere solo riletta.

investigazione attraverso un indirizzo Internet prestabilito tramite la rete Internet ed in modalità nascosta e protetta[310]. In tal caso, più che di "captatore" bisognerebbe più specificatamente parlare di "copiatore informatico"[311].

Attraverso i programmi spia che realizzano la c.d. *online surveillance*, invece, è possibile monitorare il flusso di dati che coinvolgono un determinato sistema informatico o telematico[312]. In particolare, se il dispositivo è collegato ad altri dispositivi attraverso una rete domestica o aziendale o se, comunque, il computer è connesso ad Internet, attraverso tale software è possibile monitorare tutti i dati relativi alle sue comunicazioni con la rete medesima (ora e durata della connessioni, invio e ricezione di e-mail, chat, siti Internet visitati, files scaricati, ecc.). Con riferimento a tale tipologia di programma, sarebbe più corretto parlare di "appostamento informatico"[313].

Inoltre, attraverso alcune tipologie di programmi -a metà strada tra "copiatori" e "captatori"- è possibile monitorare in tempo reale tutto ciò che viene visualizzato sullo schermo (*screenshot*), digitato attraverso la tastiera (*keylogger*), detto attraverso il microfono o visto tramite la webcam del sistema target controllato[314].

Saranno oggetto del prossimo capitolo le ipotesi, non prive di problemi interpretativi, di attività investigative che si sostanziano in intercettazioni telematiche o ambientali ovvero nella realizzazione di videoriprese: nel primo caso (intercettazioni), l'attività di ricerca della prova è tipica, perché prevista nel codice di rito *ex* artt. 266 e ss.; nel secondo caso (videoriprese), la soluzione viene dal diritto vivente che, quantomeno con riferimento al domicilio privato, distingue tra prova atipica e prova incostituzionale a seconda che le

---

[310] Si tratta della c.d. *one-timecopy* dei dati informatici presenti in un determinato momento in un sistema informatico.

[311] Così fa, ad esempio, M. TROGU, *Sorveglianza e "perquisizione" on line su materiale informatico*, cit., p. 442.

[312] Un sistema informatico è costituito da un computer in grado di elaborare dati in *input* per fornire informazioni in *output*. Due computer collegati tra loro in rete in modo tale da potersi scambiare tali dati costituiscono un sistema telematico.

[313] M. TROGU, *Sorveglianza e "perquisizione" on line su materiale informatico*, cit., p. 445.

[314] I *keylogger software*, ad esempio, consentono di creare dei file di *log* contenenti tutto ciò che viene digitato attraverso la tastiera (fisica o virtuale) del dispositivo. Tale file può essere visualizzato in tempo reale o acquisito in differita, da remoto, da parte del soggetto controllore. In alternativa, gli stessi dati possono essere captati durante la loro trasmissione attraverso uno *sniffer*, ovvero *software* che catturano i pacchetti di informazioni in una rete di computer e possono essere utilizzati per monitorare il funzionamento del sistema e/o scoprire nomi utenti e *passwords*. Così, R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online* durchsuchung, cit., p. 697. In realtà, le modalità tecniche per effettuare *online search* o *online surveillance* sono molteplici. Cfr., in particolare, M. HANSEN - A. PFITZMANN, *Techniken der Online Durchsuchung: Gebrauch, Missbrauch, Empfehlungen*, in F. ROGGAN (Hrg), *Online Durchsuchungen: Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils*, Bwv Berliner-Wissenchaft, Auflage, 2008, pp. 131 e ss.

videoriprese abbiano, o meno, contenuto comunicativo[315]. Il problema, per tornare a noi, si pone quando il software viene utilizzato per carpire informazioni dal contenuto non strettamente comunicativo, come, ad esempio, il contenuto di un file di word scritto e poi cancellato dall'utente prima di essere salvato sull'hard disk[316].

Ciò premesso con riferimento all'aspetto tecnico-operativo, è necessario ora valutare, dal punto di vista giuridico, la legittimità o meno di questo strumento investigativo. L'esito di tale valutazione ha, com'è ovvio, delle conseguenze processuali rilevanti in punto di utilizzabilità del materiale probatorio acquisito.

2. Il punto di vista tecnico-giuridico

La questione della legittimità dei nuovi *investigative tools* e dei loro limiti viene solitamente affrontata in base ad uno schema logico-argomentativo -imposto dal principio di "legalità temperata" delle prova vigente nel nostro sistema processuale- che consta di tre livelli caratterizzati da un rapporto di stretta propedeuticità[317].

Il primo livello consiste nella verifica della effettiva "atipicità" dello strumento investigativo: individuare un modello tipico in cui ricondurre le perquisizioni *online*, infatti, significherebbe risolvere *ex lege* quella valutazione di legittimità dello strumento investigativo che, altrimenti, è rimessa totalmente all'interprete.

Solo l'esito negativo di tale preliminare riscontro di tipicità consente di passare al livello successivo, consistente nella valutazione della possibilità di sfruttare, o meno, l'art. 189 c.p.p. per legittimare il mezzo atipico di ricerca della prova: l'applicabilità della norma dedicata dal codice di rito alle «prove non disciplinate dalla legge» dipende, innanzitutto, dal rispetto dei requisiti sostanziali e processuali che tale disposizione prevede.

L'ultimo livello della nostra analisi è il più impegnativo e consiste nella verifica della esistenza, o meno, di eventuali limiti di natura costituzionale. Come noto, infatti, il primo presupposto di validità di una prova atipica è la sua legittimità costituzionale. Occorre, quindi,

---

[315] Cfr. Cass., sez. un., 28 marzo 2006, Prisco, cit., p. 1347.

[316] Programmi, in sostanza, in grado di copiare sia i documenti informatici già formati e custoditi all'interno della memoria del computer, sia i dati e i documenti in formazione, copiandoli contestualmente alla loro elaborazione.

[317] G. DI PAOLO, *"Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Padova, 2008, p. 252; C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007, pp. 274 e ss.

individuare il "tipo" di bene giuridico attinto dal mezzo investigativo qualificato come atipico, onde verificarne "rango" ed "intensità" di compressione.

2.1 Tipicità o atipicità?

Andando "alla ricerca della tipicità" all'interno del codice di rito, le perquisizioni *online*, in quanto "mezzi di ricerca della prova" possono essere accostate e confrontate con le perquisizioni (ex artt. 247 e ss. c.p.p.), con le intercettazioni (ex artt. 266 e ss. c.p.p.) e, infine, con le ispezioni (ex artt. 244 e ss. c.p.p.). Ciò allo scopo di segnalarne affinità e differenze, giungendo alla conclusione, che qui si anticipa, che nessuno degli strumenti normati è in grado di fornire "copertura normativa" al c.d. captatore informatico.

Rispetto alle perquisizioni tradizionali, quelle *online* mantengono impropriamente solo il nome, in quanto ne differiscono sia per quanto riguarda il "fine", sia per quanto attiene le "garanzie" dei soggetti coinvolti. Con riferimento al primo aspetto, è facile osservare che le perquisizioni tipizzate nel codice di rito agli artt. 247 ss. sono strutturalmente orientate alla ricerca del corpo del reato[318] o delle cose pertinenti al reato[319], tant'è vero che tale attività di ricerca, in caso di esito positivo, sfocia nell'atto tipico ed irripetibile del sequestro a scopo probatorio; le perquisizioni *online*, invece, prescindono dalla ricerca del corpo del reato o delle cose ad esso pertinenti e sono finalizzate all'acquisizione di elementi utili ai fini investigativi in un contesto spazio-temporale molto più ampio e indefinito: l'attività di captazione non sfocia nell'atto tipico del sequestro, bensì in un atto atipico, probabilmente un "verbale di operazioni compiute". Quanto alle garanzie soggettive, mentre le perquisizioni tradizionali sono sì atti a sorpresa, ma ontologicamente palesi e quindi sempre e comunque conoscibili dal soggetto attinto dalla misura, le perquisizioni *online* sono atti di indagine che, per essere fruttuose dal punto di vista investigativo, devono restare ignote all'indagato durante tutto il corso del loro svolgimento. Non è una differenza di poco conto: nel primo caso, il soggetto indagato ha diritto alla notifica del decreto motivato, ha diritto di nominare e farsi

---

[318] «Con l'espressione "corpo del reato" l'art. 253 comma 2 c.p.p. indica le cose sulle quali cade la condotta criminosa (ad esempio l'atto pubblico alterato) o mediante il quale il reato è stato commesso (come l'arma omicida) nonché le cose che ne costituiscono il prodotto (come le banconote contraffatte), il profitto (si pensi alla refurtiva) o il prezzo (è il caso del denaro consegnato nella corruzione del pubblico ufficiale)». Così, P. FELICIONI , *Le ispezioni e le perquisizioni*, cit., p. 99.

[319] «In dottrina si è definita la cosa pertinente al reato come *res* con attitudine probatoria, caratterizzata da due elementi, uno sostanziale e uno processuale: la relazione con il reato e la necessarietà o utilità per l'accertamento dei fatti. Cosa pertinente al reato, quindi, è qualunque *res* idonea a provare». *Ibidem*, p. 100.

assistere da un difensore (di fiducia o d'ufficio), il quale a sua volta potrà visionare gli atti depositati presso la cancelleria del p.m.[320]; nel secondo caso, invece, tutto si svolge all'insaputa dell'indagato, il quale non ha la possibilità di esercitare alcun diritto difensivo in merito allo svolgimento delle operazioni di captazione.

Risolto negativamente il tentativo di ricondurre le perquisizioni *online* nell'alveo di tipicità tracciato dagli articoli del codice di rito dedicati alle perquisizioni tradizionali è quindi possibile cercare un accostamento con le intercettazioni di comunicazioni informatiche o telematiche, *ex* art. 266-*bis* c.p.p. La principale similitudine tra perquisizioni *online* ed intercettazioni telematiche è rappresentata dalla segretezza dell'attività di indagine: in entrambi i casi, infatti, siamo di fronte ad atti investigativi che trovano la loro ragion d'essere pratica nella possibilità di essere svolte all'insaputa dell'indagato. Ma questo è tutto. Al di là di questo punto di contatto, i due strumenti in esame differiscono ampiamente in ragione del contenuto della ricerca a cui sono rispettivamente preordinati. Le intercettazioni consistono nella «captazione, ottenuta mediante strumenti tecnici di registrazione, del contenuto di una conversazione o di una comunicazione segreta in corso tra due o più persone, quando l'apprensione medesima è operata da parte di un soggetto che nasconde la sua presenza agli interlocutori»[321] e possono avere ad oggetto: a) conversazioni o comunicazioni telefoniche, nonché altre forme di telecomunicazione (art. 266 c.p.p.); b) il flusso di comunicazioni relativo a sistemi informatici o telematici o intercorrente tra più sistemi (art. 266-bis c.p.p); c) le comunicazioni o conversazioni tra presenti (art. 266, comma 2, c.p.p.). Le perquisizioni *online*, invece, non sono finalizzate ad intercettare informazioni aventi un contenuto comunicativo (o, quantomeno, non solo), ma sono funzionali alla sistematica o periodica raccolta di dati presso il sistema informatico utilizzato dall'indagato[322], consentendone altresì la registrazione dei movimenti sul *web*[323]. Con una precisazione: ove le perquisizioni *online* fossero utilizzate per captare comunicazioni tra utenti (email, chat, ecc.), *nulla quaestio* circa la loro riconducibilità al regime giuridico delle intercettazioni, con conseguente necessaria applicazione delle forme e dei limiti per queste ultime previste[324]. Quando, tuttavia,

---

[320] Cfr. Cass., sez. un., 23 febbraio 2000, n. 7, Mariano, in *Cass. pen.*, 2000, p. 2225.
[321] Così, Cass., sez. un., 28 maggio-24 settembre 2003, Torcasio, in *Guida dir.*, 2003, 42, p. 49.
[322] *On line search*.
[323] *On line surveillance*.
[324] In realtà, sulla difficoltà di inquadramento della disciplina in tema di apprensione delle email, cfr.: E. M. MANCUSO, *L'acquisizione delle e-mail*, cit., pp. 53 e ss.; F. ZACCHÉ, *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.*, 2013, n. 4, p. 106; F. M. MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, p. 1261.

l'apprensione ha ad oggetto dati aventi carattere "non comunicativo", stante l'indiscusso arresto della giurisprudenza di legittimità, è da escludere l'inquadramento di tale attività nell'ambito proprio delle intercettazioni.

Passando al confronto tra perquisizioni *online* e ispezioni, la differenza appare evidente sotto il profilo delle finalità dei due istituti: le ispezioni sono strutturalmente finalizzate a fotografare una situazione di fatto suscettibile di irreversibile modifica; le perquisizioni *online* hanno un fine completamente diverso, che consiste nella raccolta occulta di dati e informazioni di pertinenza dell'indagato. Ancora una volta, da una parte (nelle ispezioni) abbiamo sorpresa ma conoscibilità, nonché istantaneità, dall'altra (nelle perquisizioni *online*) segretezza e periodicità.

2.2 Sull'art. 189 c.p.p.

Risolto negativamente il pur doveroso tentativo di collocare l'istituto all'interno del "tipico", l'unica alternativa, al fine di dare cittadinanza all'interno del nostro ordinamento processuale penale al c.d. "captatore informatico" è quella di "sfruttare" la norma del codice di rito dedicata proprio alla prova atipica, e cioè l'art. 189 c.p.p.[325].

Come noto, tale disposizione rappresenta la sintesi compromissoria di un vigoroso dibattito emerso ben prima dell'entrata in vigore del codice di procedura penale del 1988 tra i patrocinatori della tassatività[326] e i sostenitori della libertà dei mezzi di prova[327]. Il legislatore

---

[325] Sul tema della prova atipica, cfr. P. TONINI - C. CONTI, *Il diritto delle prove penali*, cit., p. 185 e ss.; A. LARONGA, *Le prove atipiche nel processo penale*, Padova, 2002, pp. 6 e ss.; G. TABASCO, *Prove non disciplinate dalla legge nel processo penale, Le "prove atipiche" tra teoria e prassi*, Napoli, 2011, p.13 ; G. CONSO – V. GREVI , *Compendio di procedura penale*, Padova, 2010, p. 306; G. F. RICCI, *Le prove atipiche*, Milano, 1999, p. 46 e ss.; M. TARUFFO, *Prove atipiche e convincimento del giudice*, in *Riv. dir. proc.*, 1973, p.395; Id, *La prova dei fatti giuridici. Nozioni generali*, Milano, 1992, pp. 401 e ss.; M. NOBILI, *sub. art. 189 c.p.p.*, in M. CHIAVARIO (coordinato da), *Commento al nuovo codice di procedura penale*, vol. II, Torino, 1990, p. 398; E. AMODIO, *Libero convincimento e tassatività dei mezzi di prova: un approccio comparativo*, in *Riv. it. dir. proc. pen.*, 1999, p. 3; C. PANSINI, *E' valida la prova atipica senza la preventiva audizione delle parti?*, in *Dir. pen. proc.*, 1997, p.1257; V. BOZIO, *La prova atipica*, in P. FERRUA - E. MARZADURI – G. SPANGHER (a cura di), *La prova penale*, Torino, 2013, p.57 e ss.; M. CONTE – M. GEMELLI – F. LICATA, *Le prove penali*, Milano, 2011, p.35 e ss.; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007, p.108.

[326] «Quando il codice nella sua ben architettata struttura prevede un quadro di mezzi di prova, è intorno ad esso che deve roteare la vicenda giudiziaria; essendo evidente, tra l'altro, che la mancata previsione di un mezzo di prova sta a significare che le prospettive di politica criminale che hanno presieduto alla formazione della legge lo hanno escluso; e che anche in caso di sopravvenuto delinearsi di un nuovo strumento di acquisizione della prova non è l'interprete, bensì il legislatore a dover aggiornare il sistema». Così, G. LEONE, *Trattato di diritto processuale penale*, cit., p. 178. La preoccupazione nell'ammettere prove extra catalogo legale era di veder compromessi in tal modo i diritti dell'imputato. Cfr. E. ZAPPALÀ, *Il principio di tassatività dei mezzi di prova nel processo penale*, Milano, 1982. pp. 99 e ss.; G. CONSO, *La natura giuridica delle norme sulla prova nel processo penale*, in *Riv. dir. proc.* , 1970, p.20.

del 1988 si è posto in una posizione intermedia: nel progetto preliminare del nuovo codice di procedura penale, di cui alla legge delega n. 81 del 16 febbraio 1987, decideva di non confinare i mezzi di prova entro un catalogo già tipizzato, bilanciando però tale scelta con il contestuale ampliamento delle garanzie difensive dell'imputato. Attraverso l'art. 189 c.p.p., seppur a determinate condizioni, veniva quindi introdotta la possibilità di acquisire prove non disciplinate dalla legge[328].

Tale disposizione è stata pensata dal legislatore del 1989 come "valvola di sicurezza" di cui servirsi per convogliare il progresso scientifico all'interno del processo penale, evitando «eccessive restrizioni ai fini dell'accertamento della verità, tenuto conto del continuo sviluppo tecnologico che estende le frontiere dell'investigazione, senza mettere in pericolo le garanzie difensive»[329]. Nonostante la "cautela" del legislatore codicistico, appare abbastanza evidente

---

[327] Nell'ambito di questo orientamento, favorevole alla apertura del catalogo legale, convivevano però due diverse correnti. Quella più legata ad una visione autoritaria del processo penale affermava che i vincoli probatori in materia penale dovevano considerarsi mere eccezioni ed essere pertanto rigidamente contenuti in quanto potenzialmente pregiudizievoli per l'accertamento della verità: «nel nostro processo, solidamente fondato sul principio della verità materiale vige l'obbligo della ricerca della verità stessa, onde le limitazioni legali hanno solo significato di eccezione […]; ciò che si intende di stabilire, con proclamare la libertà dei mezzi di prova, questo è, che il giudice e gli organi di prova possano ricercare la verità con tutti i più moderni mezzi che la scienza man mano progredendo suggerisca. In altre parole, le operazioni nelle quali il mezzo di prova si concreta non hanno limiti né modi assolutamente prefissati nella legge». Così, E. FLORIAN, *Delle prove penali*, III ed., Milano, 1961, p.8. Accanto a tale visione se ne sviluppò un'altra, parimenti favorevole all'apertura del catalogo legale ma più garantista, secondo cui il principio di atipicitaà probatoria doveva essere raccordato alla fissazione da parte del legislatore di vincoli probatori ben definiti che tracciassero il confine del materiale utilizzabile per la decisione: «..è prova ogni segno utile al lavoro storico giudiziario, in quanto non ne sia esplicitamente vietata l'acquisizione né ripugni a canoni enucleabili dall'intero contesto normativo: che il codice non esaurisca l'universo dei possibili segni, escludendo quanto non nomina, dipende da assennata autodisciplina....». Così, F. CORDERO, *Guida alla procedura penale*, Torino, 1986, p. 338; ID, *Tre studi sulle prove penali*, Milano, 1963, p. 64; M. CAPPELLETTI, *La natura delle norme sulle prove*, in *Riv. it. dir. proc. pen.*, 1969, p. 95.

[328] Nella sua prima stesura, l'art. 189 c.p.p. disponeva: «Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento della verità e non pregiudica la libertà morale della persona. Con il provvedimento di ammissione il giudice fissa le modalità di assunzione della prova". Successivamente, nel testo definitivo del c.p.p., emanato con D.P.R. n.447 del 22.9.1988, l'espressione "accertamento della verità" veniva sostituita con quella presente di "accertamento dei fatti" e nell'ultimo comma dell'art. 189 c.p.p. veniva aggiunta la locuzione "sentite le parti" con riferimento alle modalità di assunzione della prova atipica, ciò in ossequio al principio del contraddittorio nella formazione della prova che veniva a caratterizzare il nuovo codice di procedura penale.

[329] «L'art. 189 regola l'assunzione delle prove non previste espressamente dalla legge, così lasciando intendere che il sistema non recepisce il principio di tassatività senza peraltro ignorarne la portata garantistica. Il Progetto del 1978 aveva invece escluso l'utilizzabilità di prove atipiche od innominate nell'intento di rafforzare le garanzie difensive dell'imputato in relazione a mezzi di accertamento dei fatti di reato la cui acquisizione potrebbe condurre ad errori o abusi (ad es. tavole d'ascolto idonee ad intercettare conversazioni tra presenti). Riesaminatosi il problema in tutti i suoi profili di politica e tecnica processuale, si è scelta una strada intermedia che consente al giudice di assumere prove non disciplinate dalla legge ma lo obbliga a vagliare, a priori, che queste siano, al tempo stesso, affidabili sul piano della genuinità dell'accertamento e non lesive della libertà morale della persona. Verificata l'ammissibilità del mezzo di prova atipico, il giudice dovrà poi regolarne in concreto le modalità di assunzione così da rendere conoscibile in anticipo alle parti l'iter probatorio». Cfr. *Relazione al progetto preliminare del codice di procedura penale del 1988*, in Gazz. Uff., 24 ottobre 1988 n. 250, suppl. ord. n.2, p.60. In tema v. anche V. GREVI - G.P. NEPPI MODONA, *Introduzione al progetto*

che con l'introduzione dell'art. 189 c.p.p. sia stato abbandonato il principio di tassatività dei mezzi di prova[330], a favore di una "apertura controllata" del catalogo legale veicolata sui binari dell'idoneità probatoria[331], della tutela della libertà morale della persona[332] e del rispetto del principio del contraddittorio nella formazione della prova[333].

Ciò doverosamente premesso, la possibilità di ricorrere a tale disposizione per risolvere la questione della legittimità del captatore informatico è tutt'altro che scontata, riscontrandosi a tal riguardo opinioni contrastanti. Il tema rinvia ad una problematica più generale, sulla quale si discute ormai da tempo, senza peraltro giungere a risultati unanimamente condivisi: la configurabilità o meno, accanto ai mezzi di prova atipici, della diversa categoria concettuale dei mezzi di ricerca della prova atipici.

In base ad una prima opinione, l'art. 189 c.p.p. è applicabile esclusivamente ai mezzi di prova e non anche ai mezzi di ricerca della prova, tra i quali, evidentemente, si colloca il captatore informatico. Ciò in quanto, la norma *de qua* prevede un contraddittorio tra le parti, davanti al giudice, sulle modalità di assunzione della prova, il che la rende logicamente incompatibile con gli atti di indagine (tra i quali rientrano, secondo l'*id quod plerumque*

---

preliminare del 1988, in *Il nuovo codice di procedura penale dalle leggi delega ai decreti delegati*, vol. IV, Padova, 1990, p. 553; M. NOBILI, *La nuova procedura penale. Lezione agli studenti*, Bologna, 1989, p. 100.

330 Così, P. TONINI, *La prova penale*, Milano, 2002, p. 92. *Contra*, A. CIAVOLA, *Prova testimoniale e acquisizione per suo tramite del contenuto delle intercettazioni telefoniche*, in *Cass. pen.*, 2000, p. 488, secondo cui proprio l'art. 189 c.p.p. dovrebbe considerarsi norma posta a chiusura della disciplina del mezzi di prova.

331 L'ammissibilità della prova atipica dipende, innanzitutto, dalla capacità dello strumento probatorio di offrire un contributo utile alla ricostruzione dei fatti, contributo che non sarebbe altrimenti raggiungibile attraverso i mezzi di prova tipici. Tale prognosi di idoneità probatoria, risolta positivamente dal legislatore con riferimento ai mezzi di prova tipici, nei mezzi di prova atipici è onere del giudice e si traduce in un giudizio di "non manifesta inidoneità" del mezzo di prova atipico a verificare i fatti per cui si procede. Cfr. O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, cit., p.225 e ss.; G. TABASCO, *Prove non disciplinate dalla legge nel processo penale*, cit., p.52. C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p.116 che precisa come «la preminenza accordata a tale primo requisito non è casuale perché questo rappresenta un *prius* logico anche rispetto alla verifica della compatibilità (della prova atipica) con la libertà morale».

332 Tale requisito si identifica con il dovere di garantire ai soggetti coinvolti dall'utilizzo dello strumento atipico il diritto di autodeterminarsi rispetto agli stimoli esterni e si traduce nel divieto di utilizzare, «neppure con il consenso della persona interessata, metodi o tecniche idonei ad influire sulla libertaÌ di autodeterminazione o ad alterare la capacitaÌ di ricordare e di valutare i fatti» (art. 188 c.p.p.). Sulla differenza tra libertaÌ personale intesa come assenza di coercizioni fisiche e libertaÌ morale, intesa come assenza di coercizione psichica idonea a pregiudicare la capacitaÌ di autodeterminazione del soggetto, v. G. VASSALLI, *La libertaÌ personale nel sistema delle libertaÌ costituzionali*, in Id., *Scritti giuridici*, vol. III, Milano, 1997, p.177 e ss.

333 Nel caso si debba assumere una prova non disciplinata dalla legge il contraddittorio viene garantito non solo nel momento della formazione della prova, ma ancor prima, nel momento di individuazione del procedimento acquisitivo, non essedo quest'ultimo tipizzato nel codice di rito. Cfr., A. LARONGA, *Le prove atipiche nel processo penale*, cit., p. 123; V. BOZIO, *Le prove atipiche*, cit., pp. 74 e ss. Il giudice non è comunque vincolato a tener conto dei suggerimenti espressi dalle parti sulle modalità di assunzione della prova atipica. Infatti solamente la mancata audizione delle stesse in contraddittorio sarebbe causa di nullità *ex* art. 178 lett. b) o c) c.p.p. Sul punto, C. PANSINI, *E' valida la prova atipica senza la preventiva audizione delle parti*, cit., p. 1258.

accidit, i mezzi di ricerca della prova), i quali avvengono in una fase preliminare, quella delle indagini preliminari, inconciliabile con qualsiasi preventiva *discovery*[334]. Pertanto, si afferma, sarebbe impossibile dare attuazione all'art. 189 c.p.p. nella parte in cui impone che il giudice senta le parti sulle modalità di assunzione della prova atipica prima di decidere con ordinanza sulla richiesta di ammissione.

Tuttavia, la dottrina maggioritaria[335] e la giurisprudenza di legittimità, nella sua composizione più autorevole[336], hanno affermato che è ben possibile ipotizzare mezzi di ricerca della prova atipici, attraverso una interpretazione "adeguatrice" dell'art. 189; secondo tale orientamento, qualora l'atipicità riguardi mezzi di ricerca e non mezzi di prova, anziché configurare un contraddittorio anticipato sulla ammissione nel corso delle indagini[337], si potrà e dovrà svolgere in dibattimento un contraddittorio posticipato sulla utilizzabilità degli elementi acquisiti[338]. Ciò in quanto «il contraddittorio previsto dall'art. 189 non riguarda la ricerca della prova, ma la sua assunzione e interviene dunque, come risulta chiaramente dalla disposizione, quando il giudice è chiamato a decidere sull'ammissione della prova»[339]. In altre parole, facendo riferimento a categorie tradizionali e distinguendo correttamente tra ricerca, ammissione, assunzione e valutazione della prova[340], potrà essere fatta applicazione dell'art. 189 anche in ipotesi di utilizzo, da parte degli inquirenti, di strumenti atipici di ricerca della prova. In tale evenienza, infatti, il contraddittorio, necessariamente successivo, non riguarderà l'attività di ricerca della prova, ma le modalità di assunzione del relativo elemento, sulle quali

---

[334] G. RICCIO, *Presentazione*, in A. FURGIUELE, *La prova per il giudizio nel processo penale*, Torino, 2007, p. 12; A. LARONGA, *L'utilizzabilità probatoria del controllo a distanza eseguito con sistema satellitare g.p.s.*, in *Cass. pen.*, 2002, p. 3058; V. BOZIO, *La prova atipica*, cit., p. 75; N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Padova, 1992, p. 213.

[335] P. TONINI – C. CONTI, *Il diritto delle prove penali*, cit., p. 187; V. GREVI, *Prove*, in G. CONSO - V. GREVI (a cura di), *Compendio di procedura penale*, Padova, 2006, p. 296; V. BONSIGNORE, *L'acquisizione di copie in luogo del sequestro: un atto atipico delle garanzie difensive*, in *Cass. pen.*, 1998, p. 1504 e ss.; M. NOBILI, *sub. art. 189 c.p.p.*, cit., p. 398; G. BORRELLI, *Riprese filmate nel bagno di un pubblico esercizio e garanzie costituzionali*, in *Cass. pen.*, 2001, p. 2446.

[336] Cass., sez. un. 28 marzo 2006, Prisco, cit., p. 1347, che hanno ritenuto ammissibili come prove atipiche le videoriprese di comportamenti non comunicativi effettuate dalla polizia giudiziaria nei luoghi cd. riservati. Cfr., inoltre, Corte cost., 4 dicembre 2009, n. 320, in *Giur. cost.*, 2009, p. 4822. In questo senso, v. anche Cass., sez. VI, 10 novembre 2011, in *C.E.D. Cass.*, n. 251563, ed ancora, sull'attività di osservazione e pedinamento della p.g., Cass., sez. VI, 3 giugno 1998, in *Cass. pen.*, 2000, p. 689, nonché Cass., sez. II, 30 ottobre 2008, in *Guid. dir.*, 2009, n.5, p.90.

[337] Il che renderebbe evidentemente inutile l'esperimento atipico, a causa del venir meno del suo effetto più importante, ovvero l'effetto sorpresa.

[338] Cfr. P. TONINI, *Manuale di procedura penale*, cit., p. 279.

[339] Così, Cass., sez. un., 28 marzo 2006, Prisco, cit., p. 1347.

[340] Cfr. P. TONINI, *Manuale di procedura penale*, cit., pp. 239 e ss.

il giudice è chiamato a decidere, ammettendo o non ammettendo la prova a seconda che siano stati rispettati o meno i canoni previsti *ex* art. 189 c.p.p.[341]

L'interpretazione adeguatrice che si fonda sul recupero *ex post* del contraddittorio non convince una parte della dottrina, secondo la quale «la tesi che predica l'applicazione dell'art. 189 c.p.p. alla fase delle indagini, pur se animata dal condivisibile intento di recuperare delle forme di tutela per la persona sottoposta alle indagini, si rivela […] totalmente inadeguata allo scopo, ed anzi soggetta al rischio di ipocrite strumentalizzazioni»**[342]**. Ciò a causa dello svilimento della portata garantistica propria dell'art. 189 c.p.p., provocato da un recupero *ex* post del contraddittorio tutt'altro che effettivo e dall'assenza di qualsiasi controllo giurisdizionale *in itinere*[343].

Lo scrivente ritiene che la soluzione del problema passi attraverso i principi generali del sistema: l'art. 189, non a caso, è posto all'interno del Titolo I del Libro III sulle prove, e cioè tra quelle "disposizioni generali" che, salvo ipotesi di incompatibilità espressa o implicita, devono trovare applicazione trasversale all'interno del codice di rito[344]. Tale indirizzo ermeneutico coglie nel segno perché restituisce alla scienza giuridica quella identità che le è propria, la quale si caratterizza non in ragione di un'attività di esegesi meramente letterale[345], quanto, piuttosto, per quella interpretazione sistematica rispetto al diritto positivo che diventa doverosa per l'interprete. Una opzione ermeneutica che, con riferimento al caso *de quo*, si estrinseca nel riconoscimento all'art. 189 c.p.p. del ruolo di vero e proprio statuto normativo della prova atipica, sia che si parli di mezzi di prova sia che si discuta di mezzi di ricerca della

---

[341] Sostengono tale tesi, tra i tanti, A. CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove incostituzionali*, cit., p. 1192, che precisa: «.... la norma opera in due modi diversi: rispetto alle prove da formare in dibattimento il giudice dovrà sentire le parti affinché queste propongano le modalità acquisitive ritenute preferibili.....Invece rispetto alle conoscenze atipiche raccolte nella fase delle indagini preliminari ..il dibattito sulle modalità di formazione della prova assumerebbe il senso di una valutazione ed eventualmente di una critica del procedimento seguito dagli investiganti: ove il giudice, sulla base delle argomentazioni delle parti, si convincesse che l'iter di assunzione non garantisce un risultato probatorio attendibile sotto il profilo gnoseologico, rifiuterebbe l'ammissione della prova ritenendola non idonea all'accertamento dei fatti...». In tema, v. anche, F. CAPRIOLI, *Riprese visive nel domicilio e intercettazioni per "immagini"*, in *Giur. cost.*, 2002, p. 2189; L. FILIPPI, *L'home watching: documento, prova atipica o prova incostituzionale?*, in *Dir. pen. proc.*, 2001, p. 92; C. MARINELLI, *Le "intercettazioni di immagini" tra questioni interpretative e limiti costituzionali*, in *Dir. pen. proc*., 1998, p. 1270; S. LONATI, *Il contraddittorio nella formazione della prova orale e i principi della CEDU: una proposta de iure condendo*, in www.dirittopenalecontemporaneo.it, 16 luglio 2012.

[342] Cfr. S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2, 2015, pp. 760 e ss.

[343] *Ibidem*.

[344] In questo senso, V. GREVI, *Prove*, cit., p. 307, nonché G. UBERTIS, *Prova e contraddittorio*, in *Cass. pen.*, 2002, p. 1182.

[345] L'interpretazione meramente letterale delle disposizioni normative è definita «metodo primitivo» dalla Corte costituzionale nella sentenza n. 1 del 2013, disponibile integralmente su www.giurcost.org.

prova "non disciplinati dalla legge". Proceduralmente, quindi, non sembrano esserci ostacoli all'applicazione del principio del "contraddittorio postumo" anche con riferimento al mezzo atipico di ricerca della prova "captatore informatico": le modalità di captazione dei dati e delle informazioni digitali, infatti, ben potranno essere oggetto di successiva discussione tra le parti, le quali, evidentemente, potranno avvalersi dell'ausilio di esperti, in qualità di consulenti tecnici. L'estensione dell'art. 189 c.p.p. anche agli strumenti investigativi atipici potrebbe invero essere giustificata dal fatto che trattasi di regola generale in tema di prova che, quale corollario del principio di legalità processuale[346], dovrebbe valere anche nella fase delle indagini preliminari in ragione dell'estensione all'indagato, *ex* art. 61 c.p.p., delle garanzie previste per l'imputato.

Oltre all'aspetto squisitamente processuale (contraddittorio sulle modalità di assunzione), l'art. 189 richiede pur sempre il rispetto di ben precisi requisiti di natura sostanziale: idoneità ad assicurare l'accertamento dei fatti e tutela della libertà morale della persona. Sul primo requisito sostanziale della norma *de quo*, *nulla quaestio*: non è in discussione in questa sede l'idoneità del *virus* a fornire elementi probatori utili alle indagini, atteso che è del tutto evidente l'enorme potenzialità dello strumento in esame dal punto di vista investigativo,: al giorno d'oggi, l'interazione intersoggettiva, ad ogni livello (familiare, sociale, lavorativa, ecc.), così come lo sviluppo della personalità di ciascuno, non possono prescindere dall'utilizzo di dispositivi informatici; di conseguenza, il controllo di questi consente il recupero di una massa di informazioni dall'enorme importanza per gli inquirenti, in qualsiasi tipo di indagine. Quanto al secondo requisito, e cioè l'integrità della libertà morale della persona fonte di prova, ogni dubbio deve essere destituito di fondamento: proprio l'essenza "subdola", perché segreta, del captatore informatico rappresenta la maggiore garanzia dell'integrità del processo volitivo della persona, la quale, non sapendo di essere controllata, assumerà un comportamento del tutto naturale e svincolato da influenze esterne.

---

[346] Per legalità processuale (principio simmetrico a quello previsto in ambito penale dall' art. 25 comma 2 Cost.) si intende «il primato della legge nel momento del procedere» rispetto a chi è chiamato ad applicarla. Cfr., N. GALANTINI, *Considerazioni sul principio di legalità processuale*, in *Cass. pen.*, 1999, p.1989. Tale principio incorpora in sè il criterio di "tassatività-determinatezza" da cui deriva la certezza della legge processuale penale, quale argine delle distorsioni applicative della procedura penale da parte del potere giudiziario. Cfr., O. MAZZA, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, cit. Secondo quanto disposto dall'art. 111 comma 1 Cost.: «La giurisdizione si attua mediante il giusto processo regolato dalla legge». Secondo l'art. 6 comma 1 Conv. eur. dir. uomo: «Ogni persona ha diritto a che la sua causa sia esaminata imparzialmente, pubblicamente e in un tempo ragionevole, da parte di un tribunale indipendente ed imparziale, costituito dalla legge....». Il principio di legalità processuale è stato definito "principio generale di diritto" anche dalla Corte eur. dir. uomo nella sentenza 22 giugno 2000 Coeme e altri c. Belgio.

Prima di chiudere, occorre sgombrare il campo da possibili equivoci. Nella preliminare attività di individuazione dei mezzi di ricerca della prova legittimamente atipici, sia che il connotato dell'atipicità venga desunto dall'estensione della disciplina di cui all'art. 189 c.p.p., sia che esso venga ancorato ad un concetto allargato di atipicità, che caratterizza per natura le indagini preliminari *ex* artt. 55 e 348 c.p.p., l'interprete non può fare a meno di confrontarsi con le regole generali dettate dal codice di rito in materia probatoria. In altre parole, anche in assenza dell'art. 189 c.p.p. non potrebbe ipotizzarsi come legittimo uno strumento atipico di ricerca della prova inattendibile o, comunque, lesivo della libertà morale della persona. La norma sulla prova atipica dimostra tutta la sua utilità nella fase successiva, quella processuale, dove si dovrà decidere sulla utilizzabilità o meno degli elementi acquisiti: infatti, mentre il "prodotto" dei mezzi tipici di ricerca della prova viene pacificamente incanalato nel processo attraverso il paradigma normativo del singolo strumento tipico[347], è lecito dubitare della stessa utilizzabilità processuale dei risultati probatori di uno strumento di ricerca della prova atipico, a prescindere dalla successiva valutazione di tali elementi, attesa l'inesistenza di una normativa alla quale fare riferimento. E' in questa fase ed a questo scopo che si innesta l'art. 189 c.p.p., i cui i requisiti "possono" essere utilizzati come parametro di legittimità delle indagini atipiche, ma "devono" essere considerati ai fini della conseguente utilizzabilità dei risultati.

2.3 Prova atipica o prova incostituzionale?

A questo punto è necessario verificare se sussistono, o meno, ulteriori limiti di natura costituzionale[348]. Quindi, è necessario passare al terzo livello della nostra analisi, ossia alla individuazione del tipo di bene giuridico attinto dal mezzo atipico di ricerca della prova. Ciò al precipuo scopo di assegnare a tale bene un rango all'interno di una ideale gerarchia di

---

[347] Nessuno dubita, ad esempio, dell'utilizzabilità procedimentale e processuale dei verbali delle intercettazioni telefoniche o delle trascrizioni delle registrazioni, senza dover ricorrere all'esame testimoniale dell'ufficiale di polizia giudiziaria che materialmente ha "captato" le conversazioni intercettate, formando il relativo "brogliaccio di ascolto", o del perito che ha svolto le relative "trascrizioni", depositando la sua perizia. Ovviamente, i risultati di tali operazioni possono essere messi in discussione attraverso ulteriori consulenze tecniche in attuazione di quel contraddittorio sulla prova che deve caratterizzare anche la prova scientifica. Ma tale aspetto attiene al momento della valutazione della prova e non a quello propedeutico della sua ammissibilità, su richiesta di parte, dopo una ricerca legittima.

[348] «Il primo presupposto di validità di una prova atipica è la sua legittimità costituzionale. Occorre quindi verificare quali diritti fondamentali siano coinvolti in tale attività di indagine, al fine di delineare i presupposti e i confini entro cui iscrivere tale mezzo di ricerca della prova» Così F. IOVENE, *Le c.d. perquisizioni on line tra nuovi diritti ed esigenze di accertamento penale*, www.penalecontemporaneo.it, 30 novembre 2015

valori: dal posto che il bene occupa all'interno di tale scala gerarchica e dall'intensità della sua potenziale lesione dipendono la legittimità dello strumento atipico e la conseguente utilizzabilità, o meno, dei risultati con esso ottenuti[349].

Punto di partenza della nostra riflessione è che, a livello sistematico, sono ipotizzabili almeno tre livelli decrescenti di garanzie del privato di fronte a possibili atti di indagine compiuti nei suoi confronti da parte delle autorità inquirenti: ad ogni livello corrisponde un diverso *stardard* di tutela e la graduazione dipende dal rango dell'interesse in gioco.

In particolare, la limitazione della libertà personale (art. 13 Cost.), del domicilio (art. 14 Cost.) e della corrispondenza (art. 15 Cost.) per fini investigativi, di accertamento e repressione dei reati, è possibile ma solo nel rispetto della doppia riserva, di legge[350] e di giurisdizione[351]. Si tratta delle tradizionali libertà di matrice liberale-ottocentesca tutelate rispetto alle intrusioni da parte dei poteri statuali nella forma più intensa che l'ordinamento italiano conosca.

Esistono poi beni giuridici sì previsti in Costituzione, ma non assistiti dalla doppia riserva, di legge e di giurisdizione: si tratta dei c.d. "nuovi diritti", o "diritti di seconda generazione", situazioni giuridiche soggettive la cui crescente importanza rappresenta il segno tangibile dell'evoluzione della coscienze sociale. La loro copertura costituzionale viene tradizionalmente individuata nell'ambito di tutela negli artt. 2 e 3 della Carta fondamentale, con la conseguenza che essi formalmente non sono assistiti dal monopolio legislativo per quanto riguarda la previsione dei "casi" e dei "modi" di una loro eventuale compressione.

E' possibile ipotizzare, infine, situazioni nelle quali non esiste alcuna aspettativa giuridicamente azionabile da parte del privato a fronte del potere-dovere dell'autorità di indagare: si tratta di contingenze nelle quali il privato agisce in modo tale da escludere potenziali rivendicazioni di diritti, perché vi rinuncia, espressamente o tacitamente, per fatti concludenti[352].

---

[349] «Guardando al fondo del problema, pare potersi rilevare che, per stabilire se esiste o non esiste il c.d. potere istruttorio, vengono effettuate tre valutazioni caratterizzate da una forte componente di discrezionalità. Anzitutto, si individua l'interesse protetto dalla norma violata. In secondo luogo, si stabilisce il rango di tale interesse. Infine, viene ponderato il grado della lesione che detta istanza ha subito, anche nel bilanciamento con gli altri interessi rilevanti nella fattispecie». Così, C. CONTI, *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali*, cit., p. 485.

[350] Si tratta dei "casi e modi previsti dalla legge" di cui agli artt. 13, co. 1, e 14, co. 1, Cost., nonché delle "garanzie stabilite dalla legge" di cui all'art. 15, co. 2, Cost.

[351] Si tratta dell' "atto motivato dell'Autorità giudiziaria" di cui all'art. 13, co. 1, Cost., richiamato dall'art. 14, 1° co, e previsto espressamente anche nell'art. 15, co. 2, Cost.

[352] Così, ad esempio, rinuncia alla riservatezza delle comunicazioni colui il quale parla a voce alta, in pubblico, con il suo interlocutore. Rinuncia alla privacy domiciliare colui il quale lascia la finestra del proprio

2.3.1 Prova atipica e riserva di legge

A fronte di "diritti fondamentali" coperti da riserva di legge rinforzata dalla necessità, da parte del legislatore, di prevedere i "casi" e i "modi" di una loro possibile limitazione, il fine accertativo del processo penale deve viaggiare sui precisi binari tracciati dal legislatore e la rotta deve essere controllata dall'Autorità giudiziaria. Dalla teoria della c.d. "prova incostituzionale"[353] conseguono l'inammissibilità del mezzo atipico di ricerca della prova che mette a repentaglio tali diritti e, comunque, l'inutilizzabilità dei risultati con esso ottenuti. La questione merita di essere approfondita perché, in assenza di chiari riferimenti normativi, non si ha unanimità di vedute in dottrina e in giurisprudenza.

Con l'espressione "prova incostituzionale" si fa riferimento a quell'elemento di prova acquisito con modalità non disciplinate dal codice di rito e lesive dei diritti fondamentali dell'individuo, costituzionalmente tutelati[354]. Si tratta del «principio secondo il quale attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione e a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito»[355]. In altre parole, altrettanto autorevoli, "non possono validamente ammettersi in giudizio mezzi di prova che siano stati acquisiti attraverso attività compiute in violazione delle garanzie costituzionali poste a tutela dei fondamentali diritti dell'uomo o del cittadino"[356]. Ciò detto, però, all'interprete rimane il compito di individuare le norme del codice di rito che consentono l'estromissione delle prove incostituzionali dal panorama conoscitivo legittimo del giudicante. Questo non tanto e non solo in ragione di quel rigore giuridico imposto, in particolare, dal principio di tassatività, e, in generale, dal principio di legalità che permea tutto il diritto delle prove penali, ma anche e soprattutto perché compito del giurista non è quello di spiegare ciò che è giusto e ciò che non lo è, ma quello più modesto di dire ciò che è lecito e ciò che non è lecito alla luce, certo, dell'intero sistema giuridico.

---

appartamento aperto in modo tale da consentire a chiunque, senza particolari accorgimenti, di vedere cosa accade all'interno. Rinuncia alla riservatezza l'utente che inserisce proprie informazioni personali sulla pagina di un social network consentendo a chiunque l'accesso e la visualizzazione.

[353] Cfr. V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. Cost.*, 1973, p. 341.

[354] C. CONTI, *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali*, cit., p. 487.

[355] Corte Costituzionale, sent. n. 34 del 1973, in www.giurcost.org.

[356] Corte Costituzionale, sent. n. 81 del 1993, in www.giurcost.org.

Sul tema della prova incostituzionale si sono formati orientamenti contrastanti. Innanzitutto, vi è chi nega a tale concetto cittadinanza all'interno del nostro ordinamento giuridico in ragione del fatto che l'art. 189, testualmente, non impedisce l'utilizzo di prove atipiche lesive di diritti fondamentali, ma estromette esclusivamente le prove inidonee all'accertamento del fatto e quelle che pregiudicano la libertà morale della persona: quindi, in forza del principio di tassatività, l'assenza di una norma di legge ordinaria che vieti acquisizioni probatorie incostituzionali impedisce di sanzionare tali acquisizioni con la inutilizzabilità processuale dell'elemento acquisito[357]. All'interno di tale posizione esegetica, vi è poi chi, non contento del risultato ultimo cui si perviene attraverso tale interpretazione (utilizzabilità processuale del materiale raccolto in spregio dei valori fondamentali tutelati dalla Costituzione), postula l'incostituzionalità dell'art. 189 nella parte in cui non prevede i casi e i modi di limitazione dei diritti fondamentali in ipotesi di utilizzo di prove atipiche lesive di tali diritti[358].

Un differente indirizzo di matrice dottrinale, ripreso dalla giurisprudenza di legittimità nella sua composizione più autorevole, ritiene che l'inutilizzabilità della prova atipica incostituzionale deriverebbe direttamente dall'art. 191 c.p.p.: «nella categoria delle prove sanzionate dalla inutilizzabilità [bisogna ricomprendere] non solo le prove oggettivamente vietate, ma [anche] le prove formate o acquisite in violazione dei diritti soggettivi tutelati dalla legge, ed, a maggior ragione, quindi, quelle acquisite in violazione dei diritti tutelati in modo specifico dalla Costituzione. Ipotesi quest'ultima sussumibile nella previsione dell'art. 191 c.p.p., proprio perché l'antigiuridicità di prove così formate od acquisite attiene alla lesione di diritti fondamentali, riconosciuti come intangibili dalla Costituzione»[359]. Si ritiene, quindi, che «i divieti ai quali fa riferimento l'art. 191 c.p.p., comma 1, siano non solo quelli stabiliti dalle norme processuali ma anche quelli rinvenibili in altri settori dell'ordinamento, e in primo luogo nella Carta costituzionale»[360]. In altre parole, si interpreta in maniera estensiva l'espressione "divieti stabili dalla legge" prevista dall'art. 191, co. 1, c.p.p. in tema di inutilizzabilità, ragionando in questi termini: nel concetto di "legge", inteso estensivamente, rientra anche la Carta fondamentale; nel momento in cui riconosce come inviolabili alcuni diritti dell'individuo, stabilendo che eventuali limitazioni sono consentite nei soli casi e modi

---

[357] F. CORDERO, *Procedura penale*, 8ˆ ed., cit., p. 618; N. GALANTINI, voce *Inutilizzabilità*, cit., p. 700.
[358] F. CAPRIOLI, *Riprese visive nel domicilio e intercettazione "per immagini"*, cit., p. 2178.
[359] Cass. pen., 16 maggio 1996, Sala; 13 luglio 1998, Galleri; 23 febbraio 2000, D'Amuri.
[360] Cass. pen., sez. un., 28 marzo 2006, Prisco, cit.

stabiliti dal legislatore ordinario, la Costituzione fissa altrettanti "divieti probatori"; gli atti acquisitivi non espressamente previsti dalla legge, che rechino un *vulnus* ai diritti fondamentali sono vietati; la violazione di tali "divieti probatori di rango costituzionale" rinviene la sua sanzione e la sua disciplina nell'art. 191 c.p.p.[361]. I sostenitori di tale indirizzo ermeneutico parlano di interpretazione costituzionalmente orientata dell'art 191 c.p.p.[362].

Sennonché, come peraltro ammesso dalla stessa giurisprudenza di legittimità che accoglie la tesi poc'anzi esposta, «questa ricostruzione è tutt'altro che scontata perché da altra parte della dottrina si sostiene che l'art. 191 c.p.p., nel prevedere l'inutilizzabilità delle c.d. prove vietate, presuppone l'esistenza di divieti che, attenendo ad atti del procedimento, non possono che derivare da norme processuali»[363]. Quale soluzione, dunque, per conciliare esigenze di giustizia sostanziale e principio di legalità, sub-specie di tassatività?

Secondo altro filone dottrinale, è necessario «intraprendere un terzo, forse più audace, percorso ermeneutico che si fonda su di una interpretazione adeguatrice dell'art. 189»[364]. In base alla c.d. "teoria dei divieti probatori impliciti"[365], l'inutilizzabilità delle prove atipiche incostituzionali si ricava non dalla Costituzione, bensì dal silenzio della legge processuale. Di fronte ad atti acquisitivi non disciplinati dalla legge l'unica norma del codice che appare fruibile è l'art. 189 sulla prova atipica. Senonché, tale disposizione, proprio perché volta a regolare una acquisizione non preconizzabile *ex ante*, non prevede una disciplina dettagliata circa i casi e i modi con i quali l'atto lesivo può essere attuato e quindi non è fisiologicamente in grado di fungere da riserva di legge ai sensi degli articoli 13, 14 e 15 Cost. Proprio in ragione di tale silenzio, vige un "divieto implicito" che preclude l'ingresso processuale alle prove atipiche lesive di diritti inviolabili: «una lettura costituzionalmente conforme dell'art. 189 c.p.p. impone di ritenere che proprio in ragione della sua struttura, volutamente generica, la norma *de qua* risulti inidonea ad attuare la riserva di legge stabilita dalla Carta

---

[361] L.P. COMOGLIO, *Perquisizione illegittima ed inutilizzabilità derivata delle prove acquisite con il susseguente sequestro*, in *Cass. pen.* 1996, p. 1548; ID., *L'utilizzabilità "assoluta" delle prove "incostituzionali",* in *Riv. dir. proc.*, 2011, pp. 30 e ss.; L. FILIPPI, *L'home watching: documento, prova atipica o prova incostituzionale?*, cit., p. 1395; F.M. GRIFANTINI, voce *Inutilizzabilità*, in *Dir. pen. proc.*, vol. VII, Torino, 1993, p. 249.
[362] A. CAMON, *Le riprese visive come mezzo di indagine: spunti per una riflessione sulle prove incostituzionali*, cit., p. 1211.
[363] *Ibidem.*
[364] P. TONINI - C. CONTI, *Il diritto delle prove penali*, cit., p. 105.
[365] *Ibidem.*

fondamentale e precluda l'ingresso processuale delle prove atipiche lesive di diritti involabili»[366].

La conseguenza è che l'utilizzo dell'art. 189 deve essere limitato ai soli casi in cui l'acquisizione atipica non leda irrimediabilmente diritti inviolabili coperti dalla doppia riserva, di legge e di giurisdizione. Ciò in quanto, a fronte di diritti tutelati costituzionalmente dalla doppia riserva, il bilanciamento tra interessi contrapposti è di esclusiva competenza del legislatore, censurabile dal Giudice delle leggi. Si tratta di libertà fondamentali ma non intangibili, la cui compressione è monopolio esclusivo del legislatore, le cui scelte sono suscettibili di essere sindacate in base al criterio di ragionevolezza dalla Corte costituzionale.

2.3.2 Prova atipica e riserva di giurisdizione

Quando lo strumento investigativo atipico non coinvolge diritti protetti da riserva di legge rinforzata[367], il principio di proporzionalità impone la massima cautela, in nome della necessità di un equo ed imprescindibile bilanciamento degli interessi coinvolti: nella fase delle indagini preliminari, il suo svolgimento rientra tra le facoltà previste dagli artt. 55, 347 e 370 c.p.p.[368], con la necessità, tuttavia, di un previo e congruamente motivato provvedimento dell'autorità giudiziaria (quindi, anche del p.m.); in dibattimento, i suoi risultati possono essere utilizzati nel rispetto dei requisiti sostanziali di cui all'art. 189 c.p.p., previa ammissione da parte del giudice, il quale dovrà sentire le parti in contradditorio sulle modalità di assunzione[369].

---

[366] Così, C. CONTI, *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali*, cit., p. 487. *Amplius*, C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, cit., p. 172.

[367] Si tratta di beni giuridici sì previsti in Costituzione, ma non tutelati dalla riserva di legge circa i casi e i modi di una loro possibile compressione (e tuttavia "coperti", per così dire, dall'art. 2 Cost.).

[368] Cfr. Cass., sez. IV, 29 gennaio 2007, Navarro Mongort, in *Cass. pen.*, 2008, p. 1137.

[369] Come noto e già detto, l'art. 189 c.p.p. consente l'ammissibilità della "prova atipica" nel processo penale al sussistere dei seguenti presupposti sostanziali: a) idoneità ad assicurare l'accertamento dei fatti; b) rispetto della libertà morale della persona fonte di prova. Occorre, inoltre, dal punto di vista procedurale, che il giudice senta le parti sulle modalità di assunzione della prova prima di decidere con ordinanza sulla richiesta di ammissione. Quanto al primo dei due requisiti sostanziali, la prova atipica deve essere in concreto capace di fornire elementi attendibili e di permettere una valutazione sulla credibilità della fonte di prova. Rispetto della libertà morale della persona, significa evitare influenze ab extra sul processo volitivo della persona, cioè garantire la facoltà della persona di determinarsi liberamente rispetto agli stimoli. Quanto, infine, al requisito procedurale, qualora si tratti di "mezzi di ricerca della prova" atipici, anziché configurare un contraddittorio anticipato sulla ammissione nel corso delle indagini, si potrà [*rectius*, si dovrà] svolgere un contraddittorio successivo sulla utilizzabilità degli elementi acquisiti, che dipenderà dalle modalità di svolgimento del mezzo atipico sfruttato

In questi casi, in assenza di stretti vincoli costituzionali ed in mancanza di precise regole codicistiche, il bilanciamento tra opposti interessi –pur doveroso- spetta all'autorità giurisdizionale. Tutto deve essere bilanciato, in ossequio al principio di proporzionalità; solo che nella prima ipotesi –diritti coperti da riserva di legge- l'ago della bilancia è in mano al legislatore, mentre nella seconda –diritti non coperti dalla riserva di legge rinforzata- è prerogativa del giudice.

Nel nostro ordinamento giuridico, l'atto motivato dell'autorità giudiziaria rappresenta quel "livello minimo di garanzie" necessario ma anche sufficiente per garantire un giusto equilibrio tra la tutela dei diritti dei soggetti coinvolti nel procedimento penale e l'esigenza di accertamento del fatto di reato e di punizione dei colpevoli. In particolare, la teorizzazione del "livello minimo di garanzie", come vera e propria "tecnica di risoluzione dei conflitti", trova uno sviluppo progressivo nella giurisprudenza della Corte costituzionale. Punto di partenza è la importantissima sentenza n. 81 del 1993, relativa al giudizio di costituzionalità dell'art. 266 c.p.p. in riferimento all'art. 15 Costituzione. Nel caso specifico, nel corso di un procedimento penale per molestie o disturbo alle persone a mezzo del telefono, il giudice si era trovato a dover decidere circa l'ammissibilità dei tabulati contenenti informazioni relative alle telefonate effettuate dalla persona imputata a quella offesa, con specifica indicazione dei giorni e delle ore delle telefonate stesse, in considerazione del fatto che tali tabulati erano stati acquisiti, presso il gestore, con provvedimento del pubblico ministero durante le indagini preliminari senza l'osservanza delle particolari cautele assicurate dal codice di rito alle intercettazioni telefoniche. Nel dichiarare non fondata la questione di legittimità costituzionale posta dal giudice remittente, la Consulta ha chiarito che, «ferma restando la libertà del legislatore di stabilire norme di attuazione dei principi costituzionali, il livello minimo di garanzie […] –che esige con norma precettiva tanto il rispetto di requisiti soggettivi di validità in ordine agli interventi nella sfera privata relativa alla libertà di comunicazione (atto dell'autorità giudiziaria, sia questa il pubblico ministero, il giudice per le indagini preliminari o il giudice del dibattimento), quanto il rispetto di requisiti oggettivi (sussistenza e adeguatezza della motivazione in relazione ai fini probatori concretamente perseguiti)- pone un parametro di validità che spetta al giudice *a quo* applicare direttamente al caso di specie, al fine di valutare se l'acquisizione del tabulato, contenente l'indicazione dei

riferimenti soggettivi, temporali e spaziali delle comunicazioni telefoniche intercorse, possa essere considerata legittima e, quindi, ammissibile»[370].

Questo modo di procedere non è rimasto un caso isolato. Sempre con riferimento all'acquisizione di tabulati telefonici per fini di indagine, nella successiva sentenza n. 281 del 1998 la Corte costituzionale, pur auspicando «che il legislatore provveda a disciplinare in modo organico l'acquisizione e l'utilizzazione della documentazione relativa al traffico telefonico, in funzione della specificità di questo particolare mezzo di ricerca della prova, che non trova compiuto sviluppo normativo nella disciplina generale prevista dal codice in tema di dovere di esibizione di atti e documenti e di sequestro», precisa che nel caso *de quo* «il livello minimo di garanzie […] risulta allo stato rispettato per l'aspetto specificatamente dedotto della autorizzazione del pubblico ministero all'acquisizione dei tabulati»[371]. Tale "livello minimo di garanzie", chiarisce la Corte, consta di due fondamentali requisiti: un requisito soggettivo, consistente nella necessità che l'attività atipica sia stata preventivamente autorizzata attraverso un atto del pubblico ministero o del giudice; un requisito oggettivo, che si traduce nell'obbligo che tale atto autorizzativo abbia un'adeguata motivazione in relazione ai fini probatori concretamente perseguiti attraverso lo strumento atipico di indagine.

La teoria che fa leva sul concetto di "livello minimo di garanzie" deriva da una interpretazione sistematica delle norme del codice di rito dedicate specificatamente ai mezzi di ricerca della prova. Basti pensare all'artt. 253 c.p.p. (oggetto e forma del sequestro), laddove, per l'assicurazione degli elementi di prova (corpo del reato e cose pertinenti al reato) ai fini dell' "accertamento del fatto", prevede una delega in bianco all'autorità giudiziaria, la quale è tenuta, tuttavia, a motivare con decreto la limitazione dei diritti dei singoli su tali oggetti (in particolare, le ragioni della privazione fisica o anche soltanto giuridica del bene sequestrato). Con lo stesso decreto, l'autorità giudiziaria ordina l'esibizione di atti e documenti coperti da segreto d'ufficio o professionale (art. 256 c.p.p.). Non esistono "casi" e "modi" dettagliatamente descritti dal legislatore, ma solo la previsione che l'incidenza sui diritti soggettivi connessi all'espletamento di tali atti sia gestita attraverso un provvedimento giurisdizionale congruamente motivato. Quando, invece, ad essere incisi sono diritti coperti da riserva di legge rinforzata, lo standard qualitativo delle norme del codice sale

[370] Questo è il ragionamento seguito dalla Corte costituzionale con riferimento alla acquisizione dei tabulati telefonici prima della entrata in vigore del codice della privacy che ne ha compiutamente disciplinato l'utilizzazione per fini investigativi. Cfr., Corte costituzionale, sentenze n. 81 del 1993 e n. 366 del 1991, in www.giurcost.org.

[371] Cfr. Corte costituzionale n. 281 del 1998, in www.giurcost.org.

vertiginosamente: basti considerare gli artt. 273 e ss. in tema di limitazione cautelare della libertà personale, gli artt. 244 e 247 in tema, rispettivamente, di ispezioni e perquisizioni, nei quali è in gioco l'inviolabilità della persona e del domicilio, nonché gli artt. 266 e ss., dedicati alle intercettazioni di conversazioni o comunicazioni, lesive della libertà e della segretezza della corrispondenza.

Da quanto appena esposto, si può trarre una conclusione: non esiste un'unica misura di tutela; la tutela apprestata dal codice varia in ragione del bene giuridico compresso per fini investigativi; da una tutela massima (riserva di giurisdizione e riserva di legge) si passa ad una tutela attenuata (minimo livello di garanzie) realizzata attraverso il provvedimento motivato dell'Autorità giudiziaria.

2.3.3 Prova atipica in assenza di riserve

Quando, infine, l'attività investigativa atipica posta in essere per ricercare le prove non intacca alcun diritto dotato di rilevanza costituzionale, essa rientra nell'ambito delle generali attribuzioni della polizia giudiziaria, cui spetta il compito di svolgere tutti «gli atti necessari per assicurare le fonti di prova e […] quant'altro debba servire per l'applicazione della legge penale» (cfr. art. 55 c.p.p.): il *right to be left alone*, in questi casi, dipende dalla iscrizione o meno del nominativo del soggetto nel registro delle notizie di reato *ex* art. 335 c.p.p.[372]

Quindi, per lo svolgimento di questo tipo di indagine atipica non è necessario alcun provvedimento giurisdizionale. I risultati ottenuti verranno evidentemente filtrati *ex* art. 189 c.p.p. D'altronde, l'opportunità di legittimare indagini atipiche si legge a chiare lettere nella Relazione che accompagna il codice di rito. La *ratio*, ovviamente, è di evitare un eccessivo "ingessamento" dell'attività della polizia giudiziaria e del pubblico ministero, a discapito della efficienza delle rispettive indagini.

Riassumendo: a fronte di mezzi atipici di ricerca della prova il modello di tutela dipende dal bene giuridico che si ritiene inciso dall'acquisizione e la ricognizione dello stesso richiede un'attività valutativa ad altissimo tasso di discrezionalità in assenza di riferimenti di diritto positivo. Con le seguenti precisazioni: soltanto in ipotesi di compressione di un diritto fondamentale coperto dalla doppia riserva, di legge e di giurisdizione, la prova atipica è inutilizzabile; viceversa, qualora venga in gioco un diritto fondamentale non coperto da

[372] Che dipende, come noto, dall'avvenuta ricezione di una qualificata *notizia criminis*.

espressa riserva di legge circa i casi e i modi della sua limitazione, l'atipicità probatoria è consentita, purché sia assistita da un provvedimento motivato del pubblico ministero e siano rispettati i requisiti previsti dall'art. 189 c.p.p.; infine, ove non sia inciso in alcun modo un interesse degno di tutela, la prova atipica è utilizzabile secondo le regole generali, anche qualora l'acquisizione sia effettuata nel corso delle indagini preliminari su semplice iniziativa della polizia giudiziaria.

3. Il bene giuridico in gioco

Il vero problema, oggi, consiste nello stabilire "se" un'acquisizione atipica lede un diritto fondamentale, nella individuazione del bene giuridico coinvolto dall'atipica attività di indagine e nella quantificazione del "grado di lesione" raggiunto[373]. Come abbiamo visto, infatti, dal corretto "incasellamento" costituzionale dell'interesse in gioco dipende la legittimità dello strumento probatorio e la conseguente utilizzabilità dei suoi risultati.

Ebbene, nonostante le diverse conclusioni, su di un punto di partenza tutti sono d'accordo: le perquisizioni *online* incidono –quantomeno– sulla riservatezza della vita privata. Ciò premesso, sulla legittimità di tale strumento investigativo atipico, e sulla conseguente utilizzabilità degli elementi ottenuti, si riscontrano opinioni differenti.

Secondo un primo orientamento, la riservatezza della vita privata non sarebbe oggetto di autonoma e specifica tutela a livello costituzionale[374], di tal ché la sua rilevanza nella più alta delle fonti, se esiste, si deve all'art. 2 Cost. Da tale considerazione preliminare, si ricava l'inesistenza della riserva di legge rafforzata dalla necessaria previsione legislativa dei casi e dei modi di possibile limitazione del diritto. La conseguenza è la legittimità del captatore informatico, pur lesivo della riservatezza, se supportato da previo e motivato provvedimento dell'autorità giudiziaria, i cui presupposti, unitamente ai risultati probatori di tale strumento atipico, potranno essere vagliati nel contraddittorio fra le parti a norma dell'art 189 c.p.p.[375].

In base ad un secondo orientamento[376], invece, su tale conclusione, apparentemente lineare, è destinata ad incidere la Convenzione europea per la salvaguardia dei diritti

---

[373] Cfr. Cass. pen., 21 giugno 2010, Angelini, n. 23742.
[374] Cfr. E. APRILE - F. SPIEZIA, *Le intercettazioni telefoniche e ambientali,* Milano, 2004, p. 160.
[375] Cfr. Cass. pen, sez. V, 14 ottobre 2009, n. 16556, in *CED* 246954.
[376] S. MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche),* cit., pp. 2855 e ss.

dell'uomo e delle libertà fondamentali (C.E.D.U.). Il ragionamento che viene proposto è il seguente: successivamente alle c.d. sentenze gemelle della Corte costituzionale, risalenti al 2006[377], si è avuta una vera e propria rivoluzione nel sistema delle fonti di diritto interno: con le sentenze n. 348 e 349 del 2007, nonché n. 39 del 2008, la Corte costituzionale, facendo leva sull'art. 117, comma 1, Cost., ha stabilito che nell'ordinamento italiano le norme CEDU hanno rango interposto, vale a dire superiore a quello della legge ordinaria ed inferiore solo a quello delle norme costituzionali. Ove si sospetti che una norma di legge ordinaria contrasti con la CEDU –e con la giurisprudenza della Corte europea dei diritti dell'uomo, che ne è l'interprete autentico– ed ove il contrasto non sia eliminabile con gli ordinari strumenti dell'interpretazione conforme, detta norma può ed anzi deve essere sottoposta allo scrutinio del Giudice delle leggi, cui spetta appunto l'ultima decisione. «In particolare, con riferimento ai diritti fondamentali, il rispetto degli obblighi internazionali non può mai essere causa di una diminuzione di tutela rispetto a quelle già predisposte dall'ordinamento interno, ma può e deve, viceversa, costituire strumento efficace di ampliamento della tutela stessa. Se si assume questo punto di partenza nella considerazione delle interrelazioni normative tra i vari livelli delle garanzie, si arriva facilmente alla conclusione che la valutazione finale circa la consistenza effettiva della tutela in singole fattispecie è frutto di una combinazione virtuosa tra l'obbligo che incombe sul legislatore nazionale di adeguarsi ai principi posti dalla CEDU […omissis…], l'obbligo che parimenti incombe sul giudice comune di dare alle norme interne una interpretazione conforme ai precetti convenzionali e l'obbligo che infine incombe sulla Corte costituzionale - nell'ipotesi di impossibilità di una interpretazione adeguatrice – di non consentire che continui ad avere efficacia nell'ordinamento giuridico italiano una norma di cui sia stato accertato il deficit di tutela riguardo ad un diritto fondamentale»[378]. Tale "combinazione virtuosa" viene anche definita "continua e dinamica integrazione" e lo scopo del meccanismo viene individuato nella massima espansione delle garanzie, anche attraverso lo sviluppo delle potenzialità insite nelle norme costituzionali che hanno ad oggetto i medesimi diritti.

---

[377] C. cost., 24 ottobre 2007, n. 348, in *Giur. cost.*, 2007, p. 3475 ss., con nota di C. PINELLI, *Sul trattamento giurisdizionale della CEDU e delle leggi con essa confliggenti*, in *Riv. AIC*, marzo 2008; C. cost., 24 ottobre 2007, n. 349, ivi, 2007, p. 3535 ss., con nota di M. CARTABIA, *Le sentenze "gemelle": diritti fondamentali, fonti, giudici*. Precisano che norme costituzionali e norme convenzionali danno vita ad un sistema integrato di tutela dei diritti fondamentali, il quale mira alla massima espansione delle garanzie, C. cost., 26 novembre 2009, n. 311, ivi, 2009, p. 4657 ss., con nota di M. MASSA, *La "sostanza" della giurisprudenza europea sulle leggi retroattive* e C. cost. 4 dicembre 2009, n. 317, ivi, 2009, p. 4747 ss., con nota di G. UBERTIS, *Sistema multilivello dei diritti fondamentali e prospettiva abolizionista del processo contumaciale*.

[378] S. MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, cit., pp. 2855 e ss.

Seguendo tale ragionamento, in forza dell'art. 8 CEDU[379], direttamente applicabile nell'ordinamento per effetto dell'art. 117 Cost., è oggi necessaria una legge ordinaria per consentire ingerenze dei pubblici poteri nella riservatezza della vita privata delle persone, nonostante l'art. 2 Cost. nulla dica a riguardo. Ciò perché, nell'ottica delle pronunce costituzionali citate, è evidente il maggior livello di tutela che la fonte sovranazionale introduce rispetto a quella interna, che quindi subisce una "virtuosa" integrazione sul punto. D'altronde, se l'art. 8 CEDU accomuna la riservatezza della vita privata, il domicilio e la corrispondenza sotto un unico "ombrello" di tutela, prevedendo che le ingerenze nell'esercizio di questi tre beni debbano trovare un fondamento legale, c'è da chiedersi se sia razionale il comportamento di un legislatore interno che preveda i casi e i modi di intrusione solo per due di essi (segnatamente, domicilio e corrispondenza) e lasci invece piena libertà in ordine ai casi e ai modi di intrusione nel terzo (vita privata). In altri termini: la Convenzione mostra di ritenere assimilabili, per natura ed importanza, i beni della vita privata, del domicilio e della corrispondenza, tanto da assoggettarli ad un comune regime di tutela, quello della riserva di legge; differenziarne il trattamento a livello interno, riconoscendo solo a due di essi ciò che la Convenzione espressamente statuisce anche per il terzo, significa introdurre una disparità di tutela del tutto contrastante con la normativa internazionale.

La conseguenza è ovvia: le perquisizioni *online* incidono sul bene giuridico della riservatezza della vita privata, la cui lesione, alla luce del nuovo combinato costituzionale-sovranazionale, esige la predeterminazione da parte del legislatore ordinario dei casi e dei modi di aggressione di quel bene. Con conseguente inammissibilità dello strumento e, comunque, inutilizzabilità degli elementi acquisiti. I sostenitori di tale orientamento non mirano, sia chiaro, alla impermeabilità nel processo delle nuove modalità investigative; piuttosto, esigono che esse siano puntualmente normate, per elementari, comprensibili e condivisibili esigenze di garanzia. Viene avvertita l'esigenza che sia il legislatore a prevedere con ogni dettaglio possibile i casi, i modi e i tempi del bilanciamento tra libertà ed autorità, ogni qual volta il progresso tecnologico consenta nuove ed impensabili forme di aggressione a primari beni giuridici (*ratio* della riserva di legge) .

---

[379] «Diritto al rispetto della vita privata e familiare, del proprio domicilio e della propria corrispondenza. 1. Ogni persona ha diritto al rispetto della propria vita privata. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

Senonché, secondo l'interpretazione fatta propria dalla Corte di Strasburgo, affinché un'attività di indagine sia considerata "prevista dalla legge" occorre una base di diritto interno, non importa se di natura positiva o giurisprudenziale. Ergo, le conclusioni appena esposte meritano di essere rivedute.

D'altronde, anche qualora la Corte europea riscontri una violazione dell'art. 8 CEDU tale da rendere ingiustificata l'ingerenza pubblica nella sfera privata dell'individuo, ciò non comporta l'espulsione automatica del dato illegittimamente acquisito dal materiale probatorio. La Corte, infatti, ne consente l'utilizzo al ricorrere delle seguenti tre condizioni: che quella prova risulti legittima ai sensi del diritto interno (anche se questo è stato giudicato illegittimo rispetto alla CEDU); che il dato incriminato non rappresenti l'unico elemento di cui il giudice dispone (in altre parole, sono necessari ulteriori riscontri); che esso non sia ritenuto determinante ai fini della condanna nel caso di specie. Ed infatti, «ritenere sempre e comunque inutilizzabili le prove assunte in violazione della Convenzione potrebbe portare, in casi estremi, a risultati difficilmente accettabili»[380]. Non bisogna dimenticare, infatti, che «assicurare l'effettività della giustizia penale è considerata dalla Corte eur. come funzione essenziale dello stato, che giustifica la compressione delle garanzie individuali in misura anche maggiore di quanto non accada in altri ambiti»[381].

4. Dal diritto alla prassi: prova atipica o prova irrituale? Il principio di non sostituibilità

In attesa di una presa di posizione giurisprudenziale, molte Procure della Repubblica si sono dimostrate "sensibili" rispetto alla questione che stiamo affrontando ed ai connessi valori in gioco. Lo dimostra il fatto che, in ipotesi di utilizzo investigativo del captatore informatico, hanno ritenuto opportuno ricorrere "analogicamente" alla disciplina delle intercettazioni per dare allo stesso una più sicura "copertura giuridica".

---

[380] Così, A. TAMIETTI, *L'utilizzazione di prove assunte in violazione di un diritto garantito dalla Convenzione non viola l'equo processo: riflessioni sul ruolo della Corte europea e sulla natura del sindacato da essa operato in margine alla sentenza P.G. e J.H. c. Regno Unito*, in *Cass. pen.*, 2002, p. 1837.

[381] Così, S. ALLEGREZZA, *Giustizia penale e diritto all'autodeterminazione dei dati nella regione europea*, in AA.VV., *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, a cura di D. NEGRI, Roma, 2007, p. 74.

In altre parole, pur di non rinunciare alle enormi potenzialità investigative del c.d. captatore informatico, nel silenzio del legislatore, i pubblici ministeri sfruttano le disposizioni codicistiche previste per un diverso mezzo di ricerca della prova, le intercettazioni di comunicazioni o conversazioni, disciplinate *ex* artt. 266 e ss. c.p.p.

Senonché, siffatto comportamento si espone a delle riserve critiche difficilmente superabili.

Innanzitutto, da un punto di vista tecnico-operativo il "captatore informatico" (tecnica di *remote forensics*) è gestito, su delega del p.m., da tecnici nominati ausiliari di polizia giudiziaria. Ciò comporta che, spesso, l'attività dei tecnici sfugge, per sua natura, al controllo dell'autorità giudiziaria e della stessa p.g.: quanto al pubblico ministero, questi si limita ad emettere un "decreto di intercettazione" (art. 267, comma 3, c.p.p.) formalmente valido, ma carente, nella sostanza, di quelle modalità esecutive necessarie, *ex* art. 271, comma 1, c.p.p., ai fini della utilizzabilità delle intercettazioni stesse; per quanto riguarda la p.g., invece, non sempre è possibile affermare, senza il rischio di essere smentiti, che l'ufficiale di polizia giudiziaria assiste in prima persona alle operazioni di captazione svolte dal tecnico[382]. D'altro canto, l'ignoranza delle effettive modalità esecutive fa sì che gli organi inquirenti possano mantenersi estranei all'attività effettuata, talora al limite del consentito. Inoltre, mentre nel caso delle intercettazioni tradizionali è necessario, oltre all'ausilio dei tecnici, anche il contributo "terzo" del gestore telefonico (con conseguente tracciamento esterno delle operazioni), in ipotesi di captazione da remoto del contenuto di un dispositivo di memorizzazione digitale delle informazioni non è necessaria alcuna "collaborazione tecnica" ulteriore, con la conseguenza che l'attività di *remote forensics* è totalmente nelle mani del tecnico ausiliario di p.g.

Ma la critica più convincente ha natura più squisitamente tecnico-giuridica: applicando analogicamente le norme sulle intercettazioni al captatore informatico o, comunque, utilizzando la norma sulla prova atipica per offrire "cittadinanza giuridica" a tale strumento investigativo all'interno del nostro ordinamento, si finisce per confondere la prova atipica in senso proprio, o innominata, con la prova atipica in senso improprio, o irrituale. Nella prova atipica in senso proprio si utilizzano componenti non tipiche: *nulla quaestio* circa l'applicabilità dell'art. 189 c.p.p. Senonché, «oggi raramente ci si trova dinanzi ad una prova atipica nel senso descritto perché i mezzi di prova tipici sembrano idonei a raggiungere tutte

[382] Ha qualche dubbio in proposito, S. ATERNO, *Digital forensics*, cit., p. 217.

le varietà di risultati probatori. Nel sistema attuale l'atipicità consiste piuttosto nell'utilizzare componenti non tipiche all'interno di un mezzo tipico»[383]. In quest'ultima ipotesi (prova atipica in senso improprio), all'interno di un mezzo tipico, una componente è sostituita da un'altra che è caratteristica di un differente mezzo di prova[384]. A parere di chi scrive, ciò non può essere consentito in forza del "principio di non sostituibilità" tra i mezzi di prova[385].

Tale principio, unitamente alla teoria della prova incostituzionale, completa la materia dei divieti probatori ricavabili dal sistema: il versatile meccanismo della prova atipica non può essere utilizzato per superare un divieto o una inutilizzabilità speciale stabilita in relazione ad un differente strumento probatorio. In altre parole, non è consentito "spacciare" per atipico uno strumento processuale al solo scopo di aggirare regole e garanzie alle quali quel mezzo sarebbe vincolato se solo lo si chiamasse con il suo vero nome, tipico appunto. Volendo fare un paragone con il diritto penale sostanziale, viene in mente la fattispecie incriminatrice della "sostituzione di persona" di cui all'art. 494 c.p.: in ambito processuale, la sanzione che dovrebbe scattare in ipotesi di questo tipo è l'inutilizzabilità *ex* art. 191 c.p.p., per violazione del divieto (implicito) di sostituibilità.

---

[383] «In verità, la nozione di "prova atipica" non è pacifica. In una prima accezione, più radicale, è atipica quella prova che mira ad ottenere un risultato diverso da quelli perseguibili dai mezzi di prova tipizzati dal codice [prova innominata]. Oggi raramente ci si trova dinanzi ad una prova atipica nel senso descritto perché i mezzi di prova tipici sembrano idonei a raggiungere tutte le varietà di risultati probatori. Nel sistema attuale l'atipicità consiste piuttosto nell'utilizzare componenti non tipiche all'interno di un mezzo tipico». Così, P. TONINI, *Manuale di procedura penale,* cit., p. 277. Cfr. anche O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, cit., p. 90 che sottolinea come il criterio dell'atipicità dovrebbe avere ad oggetto non solo l'area del *praeter legem*, concernente ciò che non è disciplinato dal catalogo legale, ma anche la formazione di un mezzo di prova tipico in modo difforme dal modello legale, allorché le regole dettate in merito non portino ad una invalidità. V, inoltre, R. ORLANDI, *Atti e informazioni dell'autorità amministrativa nel processo penale. Contributo allo studio delle prove extracostituite*, Milano, 1992, p. 24; P. TONINI, *La prova penale*, Milano, 2000, p. 93; A. PROCACCINO, *Prove atipiche*, in A. GAITO (a cura di), *La prova penale*, vol. I, Torino, 2009, p. 268.

[384] Si tratta di una prova assunta in deroga al procedimento acquisitivo dettato dal legislatore. Cfr. P. TONINI – C. CONTI, *Il diritto delle prove penali*, cit., p. 189, nonché P. TONINI, *La prova penale*, cit., p. 94. Ancora sul punto, cfr., I. PALMA, *Considerazioni sul principio di tassatività dei mezzi di prova*, in *Riv. it. dir. e proc. pen.*, 2009, p. 404; P. P. RIVELLO, *La prova scientifica*, Milano, 2014, p.123. Molto acutamente, parla in questo caso di atipicità acquisitiva C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p. 109.

[385] «"Prova non disciplinata" è la prova ontologicamente nuova o, al più, la prova che pur perseguendo un risultato probatorio corrispondente a quello di un modello tipico si formi con modalità diverse da quelle previste dalla legge e non corrispondenti a quelle di un altro mezzo tipico. In altre parole è la prova che si forma secondo un iter di assunzione che si pone non in violazione ma al di fuori del campo di applicazione delle norme che disciplinano la materia. Al contrario, non è possibile conseguire un risultato probatorio tipico, con le forme previste per un altro mezzo nominato: cioè, non è possibile servirsi della disciplina di una prova allorché ricorrano gli estremi identificativi di un'altra fattispecie probatoria». Così, A. CIAVOLA, *Prova testimoniale e acquisizione per il suo tramite del contenuto delle intercettazioni telefoniche*, cit., p. 488. Sul tema, cfr. inoltre RAFARACI, *Ricognizione informale dell'imputato e (pretesa) fungibilità delle forme probatorie*, in *Cass. pen.*, 1998, p. 1745; C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, cit., pp. 274 e ss.; F. CAPRIOLI, *Colloqui riservati e prova penale,* Torino, 2000, p. 232; FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, p. 235.

Il principio di non sostituibilità trova riscontro sia nel diritto vivente, sia nel diritto positivo. Partendo proprio da quest'ultimo profilo, di tale principio esistono ipotesi codificate: l'art. 195, co. 4, c.p.p., sul divieto di testimonianza indiretta della polizia giudiziaria, evidentemente finalizzato ad evitare aggiramenti dell'inutilizzabilità dibattimentale delle precedenti dichiarazioni; gli artt. 202, co. 5, e 270-*bis*, co. 7, che vietano di acquisire indirettamente le notizie concernenti il segreto di Stato oggetto di testimonianza o di intercettazione[386]; l'art. 240, co. 2, dove si legge che il contenuto dei documenti illegali non può essere utilizzato; l'art. 729, co. 1-*ter*, il quale stabilisce che non possono essere in ogni caso utilizzate le dichiarazioni, da chiunque rese, aventi ad oggetto il contenuto delle rogatorie inutilizzabili; l'art. 226, co. 5, disp. att., che prevede il medesimo divieto con riferimento alle intercettazioni preventive. Ma al di là delle sopra elencate ipotesi espressamente previste nel codice, il principio di non sostituibilità -posto a presidio dei limiti invalicabili del sistema e finalizzato a stigmatizzare *escamotages* che possano vanificarne l'utilità[387]- assurge a cardine del diritto delle prove in applicazione del fondamentale canone di legalità dal quale si evince un generale divieto di aggiramenti surrettizi: «Sullo sfondo, *ca va sans dire*, si staglia l'art. 111, co. 1, Cost.»[388].

Venendo al diritto vivente, anche secondo la giurisprudenza di legittimità, quando il codice stabilisce un divieto probatorio oppure un'inutilizzabilità espressa, è vietato il ricorso ad altri strumenti processuali, tipici o atipici, finalizzati ad aggirare surrettiziamente un simile sbarramento[389]. Tale orientamento è stato progressivamente esplicitato dalla Suprema Corte, la quale ha chiarito che, in presenza di limiti probatori o inutilizzabilità espresse, è vietato il ricorso ad altri strumenti processuali, tipici o atipici, che possano comunque sortire l'effetto di aggirare le norme del codice[390]. Famosi, in particolare, sono i seguenti casi, in cui il Giudice delle leggi e la giurisprudenza di legittimità hanno fatto applicazione del principio in esame: il sequestro degli appunti predisposti dall'indagato al fine di prepararsi all'interrogatorio[391]; l'agente segreto attrezzato per il suono[392]; il sequestro della corrispondenza del detenuto[393].

---

386 C. BONZANO, *Il segreto di Stato nel processo penale*, Padova, 2010, pp. 109 e 195.
387 G. SPANGHER, *"E pur si muove": dal male captum bene retentum alle exclusionary rules,* in *Giur. cost.*, 2001, p. 2821.
388 C. CONTI, *Intercettazioni e inutilizzabilità: la giurisprudenza aspira al sistema*, in *Cass. pen.*, 2011, fasc. 10, p. 3638.
389 Cass. pen., sez. un., 24 settembre 2003, Torcasio, cit., p. 30.
390 Cfr. Cass. pen., sez. I, 25 giugno 2009, Bellocco, in CED Cass., n. 244039; Cass. pen, sez. II, 18 marzo 2008, Fiaccambrino, ivi, n. 239746.
391 Corte cost., 18 giugno 1998, n. 229, in *Cass. pen.*, 1998, n. 2847, secondo cui il sequestro di appunti difensivi dell'imputato appare «del tutto contrario alle regole del processo e direttamente lesivo di principi costituzionali.

Nel caso specifico del captatore informatico, l'utilizzo dei *virus trojan* per fini investigativi desta perplessità in ragione della eterogenea moltitudine di informazioni -di carattere "comunicativo", ma anche "non comunicativo"- potenzialmente estrapolabili attraverso questo nuovo strumento tecnologico.

Quanto alle informazioni qualificabili come "comunicazioni"[394] e ottenibili attraverso il *virus*, la copertura giuridica offerta dagli artt. 266-*bis* e ss. del codice di rito[395] sembra tenere entro i limiti già esposti *supra*.

Maggiori problemi crea, invece, il contenuto "non comunicativo" estrapolabile dagli inquirenti attraverso la captazione *online*, con particolare riferimento al contenuto dei supporti digitali e, più in generale, a tutte le attività svolte dall'utente attraverso il proprio dispositivo, senza alcuna intenzione di comunicare con terzi[396]. Probabilmente, questa tipologia di dati dovrebbe essere raccolta e conservata attraverso strumenti tipici[397]. Usare surrettiziamente la

---

Il provvedimento si risolve in una palese diretta violazione dei diritti inviolabili della persona prima ancora che del diritto all'autodifesa [tale da] comportare, oltre tutto, una surrettizia quanto censurabile lesione delle regole dettate in tema di interrogatorio dallo stesso codice di procedure penale».

[392] Con tale espressone si fa riferimento all'ipotesi in cui una persona rechi con sé apparecchi di registrazione che consentono alla polizia giudiziaria l'ascolto contestuale o differito di una conversazione. Ebbene, secondo la Consulta, quantomeno in ipotesi di ascolto contestuale, la presenza di un "terzo orecchio" occulto ad almeno uno degli interlocutori lede la segretezza della comunicazione. Pertanto, la soluzione preferibile consiste nel considerare l'atto alla stregua di un'intercettazione. Una differente interpretazione –nell'ottica della Consulta- comporterebbe l'elusione delle garanzie stabilite dal codice. Cfr. Corte cost., 30 novembre 2009, n. 320.

[393] E' il caso del pubblico ministero che, all'insaputa dell'interessato, ordina all'amministrazione penitenziaria di consegnare la corrispondenza del detenuto alla polizia, a sua volta incaricata di estrarne copia. Successivamente, le buste vengono richiuse ed inoltrate al destinatario, mantenuto all'oscuro di siffatta attività. Si tratta di un provvedimento che realizza una parziale fusione di due atti tipici (il sequestro di corrispondenza *ex* art 353 ed il visto di controllo sulla corrispondenza del detenuto, disciplinato dall'art. 18-*ter* ord. pen.), dando vita ad un ibrido *terzium genus* che finisce per eludere le garanzie tipiche di entrambi. Cfr. Cass. pen., sez. VI, 10 dicembre 2009, Giacalone, in *CED 245183*, nonché Cass. pen., sez. II, 23 giugno 2006, Rescigno, in *Cass. pen.*, 2007, p. 3800. Inoltre, la possibilità di applicare in via analogica all'attività in esame la disciplina delle intercettazioni è stata esclusa dalle Sezioni unite, udienza camerale del 19 aprile 2012, ricorrente Pasqua. In dottrina, cfr. G. ROMEO, *Le Sezioni unite sull'applicabilità delle disposizioni relative alle intercettazioni alla sottoposizione a controllo e all'acquisizione probatoria della corrispondenza epistolare del detenuto*, www.penalecontemporaneo.it, 30 novembre 2015.

[394] *Facebook*, ad esempio, offre diversi servizi di messaggistica privata. Ad aprile 2008 è stata lanciata l'applicazione Chat per scambiare messaggi in tempo reale con gli amici contemporaneamente collegati al loro profilo *Facebook*. Il 15 novembre 2010 è stato annunciato un nuovo servizio integrato di gestione dei messaggi. Tramite una sola applicazione è ora possibile gestire contemporaneamente messaggi *sms*, *chat*, *email* e normali messaggi e regolare le impostazioni della *privacy*. Dall'aprile 2011 la *chat* è stata arricchita da una funzione per effettuare chiamate vocali che permette di lasciare messaggi ad una segreteria vocale. Il 6 luglio 2011 è stato lanciato il servizio di videochiamate che utilizza la tecnologia di *Skype*.

[395] Cfr., per un approfondimento, S. DE FLAMMINEIS, *Le intercettazioni telematiche*, in *Dir. pen. proc.*, 2013, 8, p. 988.

[396] Si tratta di informazioni, spesso irrilevanti rispetto alla prova del reato per cui si procede, attinenti alla vita privata dell'indagato o di altre persone, quali abitudini, opinioni politiche e preferenze sessuali, ecc.

[397] Come già sottolineato, la legge n. 18 marzo 2008, n. 48 (di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica) ha ricondotto nell'alveo dei mezzi "tipici" di ricerca della prova la perquisizione, l'ispezione ed il sequestro di ogni sistema o supporto informatico. Per un approfondimento delle garanzie

norma sull'intercettazione telematica per fini che non le sono propri rappresenta un illegittimo aggiramento delle norme processuali poste a garanzia dell'indagato[398].

In particolare, l'utilizzo del captatore informatico per fini di perquisizione comporta l'elusione delle seguenti garanzie difensive previste per le perquisizioni tradizionali: conoscibilità dell'atto (250); assistenza del difensore (365); deposito del verbale (366); adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione (247, co. 1-*bis*).

L'ultimo aspetto citato, peraltro, fa emergere quella che potremmo definire la problematica principale che caratterizza questo nuovo strumento di indagine: come è stato rilevato in dottrina, il c.d. "captatore informatico" mal si concilia con quelle esigenze di immodificabilità e di genuinità della *digital evidence* che rappresentano una costante delle norme introdotte attraverso la legge n. 48 del 2008[399]. Ed infatti, un dispositivo digitale "aggredito" attraverso "virus di Stato" si può dire «alterato a livello strutturale e informatico»[400]. A causa del *malware*, «mutano alcune funzioni di sistema specifiche che consentono ad un operatore da remoto e connesso alla rete di prendere il possesso dello strumento e di far compiere allo strumento stesso una serie di operazioni fuori dal controllo dell'utente autorizzato modificando molte funzioni tipiche di sicurezza del sistema». C'è il rischio, inoltre, di «alterare anche accidentalmente il contenuto del sistema informatico non consentendo alla difesa di ripetere l'operazione di acquisizione»[401]. Quindi, essendo potenzialmente in grado di

---

introdotte nel codice di rito attraverso la citata legge, cfr. P. TONINI, *Manuale di procedura penale*, cit., p. 378-379.

[398] Cfr. C. CONTI - P. TONINI, *Il diritto delle prove penali*, cit., p. 106.

[399] Quanto alle ispezioni informatiche, con le modifiche aggiuntive all'art. 244 c.p.p., si è stabilito che l'autorità giudiziaria possa disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. Quanto alla perquisizione, la modifica ha interessato l'art. 247 c.p.p. al quale è stato aggiunto un nuovo co. 1 *bis*, in base al quale, ove si abbia motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, deve esserne disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. Per i casi di urgenza, è stata altresì prevista una modifica all'art. 352 c.p.p. in materia di perquisizioni, e una modifica all'art. 354, in tema di accertamenti urgenti e sequestro: le nuove norme prevedono che gli ufficiali di polizia giudiziaria adottino le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione (352) e provvedano, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità (354). Cfr. S. ATERNO, *Digital forensics*, cit., p. 217.

[400] Ibidem.

[401] *Ibidem*: «È assai discutibile sostenere […] che l'attività è sempre reiterabile in quanto è possibile compierla anche una seconda volta al momento del dibattimento. È come dire che una perquisizione domiciliare (irripetibile per eccellenza) è ripetibile "n" volte perché la difesa può tornarci quando vuole dopo che il locale è stato perquisito dalle forze di polizia. Non è proprio così o comunque non è assolutamente stato dimostrato come sia stata garantita la genuinità e integrità dei *files* acquisiti». Sulla necessità del contraddittorio se si modifica

alterare unilateralmente e senza possibilità di controllo, né *ex* ante, né *ex* post, il dispositivo "target"[402], il *trojan* di Stato appare in contrasto con le nuove norme introdotte dalla legge n. 48 del 2008.

In altre parole, mentre attraverso gli strumenti tipici previsti per l'acquisizione dell'evidenza digitale si riesce, in qualche misura, a tutelare il contraddittorio tecnico sulla prova[403], utilizzando la perquisizione a distanza questa fondamentale garanzia difensiva viene senz'altro meno. Da remoto, infatti, non c'è la possibilità di creare una copia forense del contenuto dei supporti digitali utili alle indagini, semplicemente perché il dispositivo del soggetto indagato, per ovvie esigenze di segretezza dell'indagine, non può essere cristallizzato. Da ciò deriva l'impossibilità tecnica di avere una copia dei dati conforme ad un originale che non esiste, atteso che i dati sono soggetti a continui mutamenti a seguito degli interventi manipolativi dell'ignara persona sottoposta ad indagine. In buona sostanza, nulla di ciò che viene acquisito a distanza dagli inquirenti potrà avere un termine di paragone in mano alla difesa, semplicemente perché a quest'ultima, ignara di tutto, non viene rilasciata alcuna copia dell'oggetto dell'acquisizione atipica. Diventa impossibile, quindi, garantire la genuinità del dato e la sua non modificabilità, con la conseguenza che tale acquisizione produrrà dal punto di vista probatorio dei risultati inattendibili, se non addirittura inutilizzabili[404]. Anzi, a fronte di tali attività atipiche si potrebbe addirittura parlare di "inesistenza"[405] dell'atto, con tutte le conseguenze, disciplinari[406] ma anche penali[407], di un

---

l'elemento di prova, cfr. P. TONINI, *Documento informatico e giusto processo*, cit., p. 405. Più in generale, v. P. TONINI, *Considerazioni su diritto di difesa e prova scientifica*, in *Arch. pen.*, 2011, n. 3, p. 821.

[402] Più in dettaglio, un software *trojan*, oggi è in grado di: entrare di nascosto nel sistema "target", prendendo il completo controllo di tutte le funzioni, periferiche comprese (controllo della *webcam*, navigazione, posta elettronica, microfoni; intercettare eventuali comunicazioni telefoniche o telematiche effettuate con il sistema informatico; acquisire e recapitare *online* all'investigatore, ad intervalli di tempo predefiniti a piacere o in tempo reale, tutto il contenuto del PC (ogni tipo di *file*, *log* di navigazione *web*, posta elettronica, foto, *screenshots* dei siti web visitati); autodistruggersi con un comando appositamente predisposto, pulendo le sue tracce all'interno del PC; *uplodare*, ovvero inviare e memorizzare nel sistema informatico "target" qualsiasi tipo di file, salvandolo a piacimento in qualsiasi parte del sistema.

[403] *Ex* ante, in ipotesi di copia forense realizzata *ex* art. 360 c.p.p.; *ex post*, in ipotesi di accertamento urgente eseguito *ex* art. 354 c.p.p.

[404] Si potrebbe addirittura pensare alla categoria concettuale della "inesistenza".

[405] Causa di invalidità di matrice dottrinale e giurisprudenziale, l'inesistenza si verifica tutte le volte in cui l'atto giuridico non possiede nemmeno quelle caratteristiche minime che consentono di definirlo tale. Si tratta di un «rimedio a quelle clamorose violazioni della legge processuale che non sono state espressamente previste dal legislatore proprio a causa della loro eccezionalità». Essa rappresenta una doverosa eccezione al principio di tassatività, in quanto «sarebbe profondamente ingiusto che simili vizi non potessero essere rilevati a cagione dell'impossibilità di inquadrarli all'interno di una delle cause di invalidità espressamente previste». Così, P. TONINI, *Manuale di procedura penale*, cit., p. 218 e ss., il quale, esemplificando, cita la «carenza di potere giurisdizionale in colui che ha pronunciato la sentenza, come avviene nell'ipotesi di sentenza penale emessa da un organo della pubblica amministrazione».

agire che si pone non solo al di fuori della cornice di legittimità processuale, ma anche al di là di una stretta legalità sostanziale.

Secondo una parte della dottrina[408] questa nuova tipologia di indagine potrebbe essere utilizzata quando la legge consente il ricorso al "ritardato sequestro". Il riferimento, in particolare, è al differimento del sequestro disciplinato dall'art. 9, comma 6, della legge n. 16 marzo 2006, n. 146 ed al ritardato sequestro nell'ambito di operazioni finalizzate al contrasto dello sfruttamento sessuale dei bambini e della pedopornografia (delitti di cui agli articoli 600-bis, primo comma, 600-*ter*, commi primo, secondo e terzo, e 600-quinquies c.p.[409]). Si tratta di vere e proprie scriminanti, o cause di giustificazione speciali, la cui opportunità è da rinvenire nel tentativo, da parte del legislatore, di favorire il buon esito di speciali operazioni di polizia, intraprese con l'ausilio di agenti sotto copertura, finalizzate al contrasto di delitti appannaggio di associazioni criminali sempre più complesse e difficili da smantellare[410]: una

---

[406] Cfr. art. 124 c.p.p., secondo il quale «I magistrati, i cancellieri e gli altri ausiliari del giudice, gli ufficiali giudiziari, gli ufficiali e gli agenti di polizia giudiziaria sono tenuti a osservare le norme di questo codice anche quando l'inosservanza non importa nullità o altra sanzione processuale».

[407] Cfr. art. 615-*ter* c.p.: «Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti».

[408] S. ATERNO, *Digital forensics*, cit., p. 217-247.

[409] Quanto alla prima ipotesi, nell'ambito di specifiche operazioni di polizia, il personale (ufficiali di p.g.) appartenente alle strutture specializzate della Polizia di Stato, dell'Arma dei carabinieri, del Corpo della Guardia di finanza e della Direzione investigativa antimafia, può omettere o ritardare gli atti di propria competenza, ivi incluso il provvedimento di sequestro, dandone immediato avviso al pubblico ministero e provvedendo a trasmettere allo stesso motivato rapporto entro le successive quarantotto ore. Per le stesse ragioni, il pubblico ministero può, con decreto motivato, ritardare l'esecuzione del provvedimento di sequestro. L'art. 14, comma 3, della legge n. 269 del 1998, invece, prevede che l'autorità giudiziaria possa, con decreto motivato, ritardare l'emissione o disporre che sia ritardata l'esecuzione dei provvedimenti di sequestro, quando ciò sia necessario per acquisire rilevanti elementi probatori inerenti i delitti di cui agli articoli 600 *bis*, primo comma, 600 *ter*, commi primo, secondo e terzo, e 600 *quinquies* del codice penale. Nell'ambito di questo specifico settore investigativo va rimarcata la singolare abrogazione, ad opera della l. 146/2006, della disposizione contenuta all'art. 10 della l. 419/1991 (modificata peraltro solo pochi mesi prima con legge 38/2006), che oltre a prevedere una estensione delle fattispecie criminose per i quali veniva consentito il differimento del sequestro, prevedeva, altresì, la possibilità per il p.m. di disporre, nei casi di urgenza, anche oralmente, il differimento del sequestro, salvo l'emissione del decreto entro le successive quarantotto ore.

[410] Si rinvia, per un approfondimento, al dossier edito dalla Scuola di Polizia Tributaria della Guardia di Finanza dal titolo *Tecniche investigative speciali per il contrasto patrimoniale alla criminalità organizzata*, anno di studi 2007-2008, consultabile al seguente link: *http://www.gdf.gov.it/repository/contentmanagement/information/n60984431/quaderni_21.pdf?download=1*

rigida applicazione delle norme procedurali[411] rischierebbe, infatti, di compromettere o, comunque, di contenere l'accertamento delle responsabilità penali ad un livello tendenzialmente basso[412].

Dunque, *de iure condito* sembra doversi trarre il divieto di utilizzazione dei *virus* informatici sia nell'ambito di indagini atipiche sia mediante l'impiego della disciplina delle intercettazioni: nel primo caso, osta un'interpretazione conforme all'impostazione personalistica della nostra Carta fondamentale; nel secondo caso, è di ostacolo il principio di non sostituibilità, che deriva da una esegesi puntuale delle stesse norme del codice di rito, all'indomani della novella del 2008.

5. Virus di Stato e diritto vivente: i precedenti in Italia

5.1 La sentenza "Virruso"

In Italia, i giudici di legittimità si sono occupati direttamente del fenomeno del captatore informatico soltanto in pochissime occasioni, una delle quali risale al 2010, decisa con la famosa sentenza "Virruso"[413].

Il "caso" nasce a seguito dell'utilizzo, da parte della Polizia di Stato, di un captatore informatico in grado di acquisire i files memorizzati all'interno della memoria del personal computer in uso ad uno dei principali indagati e situato presso il suo luogo di lavoro (gli uffici del depuratore di acque potabili del Comune di Villafrati). Tecnicamente, il p.m. autorizzava tale attività, in data 22.04.2004, tramite "decreto di acquisizione di atti", ai sensi dell'art. 234 c.p.p. In realtà, il decreto disponeva l'acquisizione non solo dei files già esistenti, ma, anche di tutti quei dati che sarebbero stati inseriti in futuro nella memoria del personal computer

---

411 Come noto, il sequestro del corpo del reato è un atto dovuto e, di regola, non differibile.

412 La scriminante vuole evitare che il risultato di delicate e complesse indagini, magari a livello internazionale, sia frustrato da inopportuni ed intempestivi adempimenti formali e sostanziali. Così, A. BRACCI, *Aspetti penali della disciplina delle sostanze stupefacenti e psicotrope*, in *Polizia Moderna*, suppl. al n. 5, p. 73. La stessa Suprema Corte ha ravvisato che, ove con l'acquisto simulato, che pur rappresenta il momento culminante dell'infiltrazione nell'illecito traffico, l'attività investigativa dovesse arrestarsi, verrebbe perduta l'occasione di più cospicui risultati. Cfr. Cass. pen., sez. VI, 3.12.1998, in *Cass. pen.*, 1999, 800. D'altronde, non sono infrequenti nella pratica le ipotesi in cui l'operazione sotto copertura, dopo la realizzazione della condotta tipica legittimata dalle scriminanti speciali, debba proseguire semplicemente per consentire l'allontanamento dell'infiltrato dal luogo dell'operazione per ragioni di personale incolumità.

413 Cass. pen., sez. V, 14 ottobre 2009, n. 16556, in *CED* 246954.

ritenuto in uso al soggetto indagato. Ed infatti, il captatore informatico utilizzato dagli inquirenti (*gosth*) era in grado non soltanto di copiare i files già elaborati, ma anche di registrare in tempo reale tutti i files elaborandi, realizzando in tal modo un vero e proprio monitoraggio occulto e continuativo del contenuto della memoria di massa del computer "infetto" (protrattosi per oltre otto mesi). Sulla base del materiale probatorio così acquisito, gli imputati venivano condannati, in primo grado, dal g.u.p. del Tribunale di Palermo in data 15.11.2006, avendo il giudice di prime cure ritenuto processualmente legittima l'attività investigativa posta in essere, inquadrata come prova atipica, a mente dell'art. 189 c.p.p.

In appello, la difesa sosteneva la necessaria sussunzione di siffatta attività investigativa nell'ambito applicativo proprio delle intercettazioni telematiche. La tesi era chiara: l'attività di indagine posta in essere attraverso l'installazione di un congegno di captazione in grado di registrare in tempo reale, in modo continuativo ed occulto, i flussi comunicativi generati dall'utente avrebbe dovuto essere giuridicamente qualificata come vera e propria intercettazione di comunicazioni informatiche, ai sensi dell'art. 266-*bis* c.p.p. Di conseguenza, il p.m. avrebbe dovuto richiedere l'intercettazione al g.i.p., il g.i.p. avrebbe dovuto autorizzarla con decreto motivato e il p.m., sulla scorta del provvedimento del giudice, avrebbe dovuto emettere idoneo decreto di dettaglio, contenente le modalità operative nonché la durata delle operazioni di intercettazione. Tutto ciò, nel caso *de quo*, non era in atti. Ergo, i risultati delle captazioni eseguite, nella specie, in spregio delle disposizioni degli artt. 266-*bis* e seg. c.p.p. sarebbero dovuti essere considerati come inutilizzabili a norma dell'art. 271 c.p.p. In ogni caso, si aggiungeva in quella sede, il materiale raccolto dagli inquirenti avrebbe dovuto costituire in se "prova incostituzionale" inutilizzabile a norma dell'art. 191 c.p.p., per violazione degli artt. 14 e 15 Costituzione.

La Corte di Appello di Palermo e la Corte di Cassazione non hanno accolto le doglianze della difesa. In particolare, per quello che più interessa in questa sede, i giudici di legittimità hanno escluso la riconducibilità del captatore informatico al diverso concetto di intercettazione telematica: «nella specie, l'attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull'hard disk dell'apparecchio […] aveva avuto ad oggetto non un flusso di comunicazioni, richiedente un dialogo con altri soggetti, ma una relazione operativa tra microprocessore e video del sistema elettronico, ossia un flusso unidirezionale di dati confinato all'interno dei circuiti del personal computer. Pertanto, correttamente, i giudici di merito hanno ricondotto l'attività di captazione in questione al concetto di prova atipica, sottratta alla disciplina prescritta dagli artt. 266 e ss. c.p.p.,

utilizzandone i risultati». La Corte di cassazione ha inoltre escluso che l'attività captativa *de quo* possa violare gli artt. 14 e 15 Cost.: non c'è stata violazione dell'art. 14 perché, si legge, «l'apparecchio monitorato con l'installazione del captatore informatico non era collocato in un luogo domiciliare ovvero in un luogo di provata dimora», ma nei locali sede di un ufficio pubblico comunale, dove l'imputato non godeva certamente di uno *ius escludendi alios*; non ci sarebbe stata violazione dell'art. 15, perché «quanto riprodotto in copia non era un testo inoltrato e trasmesso col sistema informatico, ma soltanto predisposto per essere stampato su supporto cartaceo e successivamente consegnato sino al suo destinatario»[414].

Su tale pronuncia sia consentita qualche riflessione.

Non desta particolari perplessità il rigetto della censura relativa alla presunta violazione dell'art. 15 Cost. (libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione) nella misura in cui, attraverso il captatore informatico, si sono acquisiti dati e informazioni di carattere non comunicativo. Posto che «per flusso di comunicazioni deve intendersi la trasmissione, il trasferimento, di presenza o a distanza, di informazioni da una fonte emittente ad un ricevente, da un soggetto ad altro, ossia il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici, non potendo ritenersi sufficiente [al fine di integrare una qualsiasi forma di comunicazione, n.d.r.] l'elaborazione del pensiero e l'esternazione, anziché mediante simboli grafici apposti su un supporto cartaceo, in un documento informatico realizzato mediante un sistema di videoscrittura ed in tal modo memorizzato»[415], ne deriva che nel caso in argomento l'attività autorizzata dal p.m. non ha avuto ad oggetto una "comunicazione" così intesa. D'altronde, il concetto di intercettazione è ormai chiaro, stante il consolidato orientamento giurisprudenziale[416] e l'unanime dottrina sul punto[417]: è intercettazione quella captazione, ottenuta mediante strumenti tecnici di registrazione, del contenuto di una conversazione o di una comunicazione segreta in corso tra due o più persone, quando l'apprensione medesima è operata da parte di un soggetto che nasconde la sua presenza agli interlocutori. Tuttavia, è appena il caso di aggiungere che la distinzione tra contenuto comunicativo e contenuto non comunicativo dei dati e delle informazioni memorizzate, in teoria limpida, non appare altrettanto scontata in concreto: basti pensare alle missive elaborate o elaborande contenute

---

[414] *Ibidem.*
[415] Cass. pen., sez. un., 23 febbraio 2000, n. 6, in *Cass. pen.*, 2000, p. 58.
[416] Cass. pen., sez. un., 28 maggio 2003, n. 36747, in *CED*. 225470.
[417] Per tutti, P. TONINI, *Manuale di procedura penale*, cit., pp. 389 e ss. Cfr. anche P. TONINI - C. CONTI, *Il diritto delle prove penali*, cit., pp. 392 e ss.

nella memoria di massa dell'indagato nel caso *de quo*, che costituiscono senza dubbio corrispondenza epistolare del soggetto, seppur solamente potenziale nel momento in cui il file viene acquisito (semplicemente per il fatto che ipoteticamente il soggetto non abbia avuto il tempo materiale per inoltrarla).

Non appare convincente, invece, né in teoria né in pratica, l'argomentazione utilizzata dai giudici di legittimità per contestare la censura relativa alla violazione dell'art. 14 Cost., che tutela, come noto, l'inviolabilità del domicilio. La Cassazione, infatti, fa rientrare nell'ambito di tutela della disposizione costituzionale in commento una definizione di domicilio limitata al mero luogo fisico di ubicazione dell'apparato informatico attinto dalla captazione[418]. Così facendo, tuttavia, la Corte confonde il luogo fisico ove è collocato il sistema informatico con il sistema informatico quale luogo, o comunque proiezione di un luogo, degno di autonoma tutela[419].

A parere dello scrivente, il bene giuridico "domicilio informatico", al pari del domicilio fisico, è tutelato dalla previsione della doppia riserva, di legge e di giurisdizione, *ex* art. 14 Cost. Tale convinzione si fonda su molteplici fattori[420].

Innanzitutto, la stessa collocazione sistematica dell'art. 615-*ter* all'interno del codice penale: tale disposizione, rubricata «Accesso abusivo ad un sistema informatico o telematico» è stata inserita dal legislatore, attraverso la legge n. 547 del 1993, fra i «Delitti contro la persona» riguardanti l'inviolabilità del domicilio, il cui referente costituzionale è proprio l'art. 14.

---

[418]«Invero, l'apparecchio monitorato con l'installazione del captatore informatico non era collocato in un luogo domiciliare ovvero in un luogo di privata dimora, ancorché intesa nella sua più ampia accezione, bensì in un luogo aperto al pubblico. Il personal computer, infatti, si trovava nei locali sede di un ufficio pubblico comunale, ove sia l'imputato sia gli altri impiegati avevano accesso per svolgere le loro mansioni ed ove potevano fare ingresso, sia pure in determinate condizioni temporali, il pubblico degli utenti ed il personale delle pulizie, insomma una comunità di soggetti non particolarmente estesa, ma nemmeno limitata o determinabile a priori in ragione di una determinazione personale dell'imputato». Così, Cass. pen., sez. V, 14 ottobre 2009, n. 16556, in *CED* 246954.

[419] Il concetto di "domicilio informatico" è stato fatto proprio ed esplicitato dalla stessa Corte di cassazione. Cfr. Cass. pen., sez. V, 26 ottobre 2012, n. 42021, in *Foro it.*, 2012, 12, 2, p. 709, dove si legge che « Con la previsione dell'art. 615 ter cod. pen., introdotto a seguito della L. 23 dicembre 1993, n. 547, il legislatore ha assicurato la protezione del "domicilio informatico" quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto».

[420] «Sul punto si rimarca l'importanza rivestita dalla sicurezza informatica, scienza che si pone in un rapporto ambivalente di rimedio-ostacolo alle procedure di informatica forense. Il punto relativo alle misure di sicurezza rende ancor più garantita la figura del "domicilio informatico" alla quale sembrano estendersi tutte le garanzie previste al "domicilio tradizionale». Così, C. MAIOLI - E. SANGUEDOLCE, *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, www.altalex.com, 30 novembre 2015.

A ciò si aggiunga quanto riportato nella Relazione che accompagna il disegno di legge che è poi sfociato nella l. n. 547 del 1993, dove si può leggere che tutte le incriminazioni di nuovo conio rispondono all'esigenza di fornire «un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'articolo 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del codice penale»[421].

Il dato testuale dell'art. 14 Cost. non deve trarre in inganno: una nozione di domicilio disancorata dalle coordinate spazio-temporali non era nemmeno prospettabile ai tempi in cui fu varata la Costituzione; ciononostante, la ratio della norma in questione oggi deve spingerci non soltanto nella direzione della tutela del domicilio fisico, ma anche e sempre di più verso la difesa di quegli spazi virtuali che rappresentano, ormai, una coniugazione fondamentale della vita dell'individuo. Tale ratio «si spiega con l'esigenza di tutelare lo jus excludendi di ciascun soggetto (pubblico o privato, persona fisica o persona giuridica) degli estranei dalla propria sfera di pensiero o di attività racchiusa nel domicilio informatico»[422]. Anzi, probabilmente, quest'ultimo può rappresentare qualcosa di ancor più personale e intimo del domicilio tradizionale, «perché mentre in questo si trovano oggetti, siano essi anche documenti o effetti personali, nel sistema informatico, sia esso depositario dell'attività lavorativa dell'individuo, o anche della sua vita privata, è custodita e conservata una estensione della nostra stessa mente, poiché l'utente, "lavorando" con la macchina, e inserendo le proprie informazioni in essa, le affida i suoi programmi lavorativi e/o personali, i suoi pensieri, i suoi progetti (passati, presenti o futuri) : tutti questi dati rappresentano tracce ed espressioni del nostro vivere quotidiano e della nostra personalità; per cui, sotto tale profilo, l'esigenza di una salvaguardia della riservatezza del domicilio informatico risulterebbe ben più rilevante ed importante dello stesso domicilio fisico, travalicando il semplice aspetto della tutela della riservatezza dei luoghi di vita della persona, ed abbracciando la tutela della stessa personalità dell'individuo»[423].

Se tale premessa viene condivisa, la conclusione è scontata: il captatore informatico è potenzialmente in grado di ledere un bene giuridico protetto dalla doppia riserva, di legge e di giurisdizione; ergo, la sua legittimità -e, di conseguenza, la utilizzabilità dei risultati con esso ottenibili- non può prescindere da una legge chiara e precisa che ne specifichi le modalità di

---

[421] In questi termini la Relazione al d.d.l. 1115/5 del 26 marzo 1993, cit. da F. MUCCIARELLI, *sub art. 4 L. 23 febbraio 1993 N.547 (Criminalità informatica)*, in *LP.* 1996, p. 98.
[422] Così G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, p. 66.
[423] In questi termini ancora G. PICA, *op. ult. cit.*, p. 66.

impiego operativo. Allo stato dell'arte, quindi, tale mezzo atipico di ricerca della prova integra una ipotesi di "prova incostituzionale"[424], stante la fisiologica inidoneità dell'art. 189 c.p.p. ad adempiere la riserva di legge *ex* art. 14 Cost. Di conseguenza, gli elementi probatori ottenuti attraverso tale strumento atipico lesivo di diritti fondamentali dell'individuo sono colpiti da inutilizzabilità, in ragione del divieto implicito nel silenzio dell'art. 189 c.p.p.[425].

Volendo, è possibile anche andare oltre il domicilio: l'utilizzo di strumenti di controllo occulto dalle potenzialità illimitate appare idoneo a determinare un mutamento qualitativo del bene giuridico aggredito. L'esperienza dei "tempi moderni" insegna che il computer è una vera e propria "appendice" della persona e dell' "io" più profondo. L'invasione in tempo reale di tali contenuti – è noto che può essere captato anche ciò che viene scritto su di un file e successivamente cancellato – sembra intaccare un bene giuridico equiparabile al domicilio, se non ancora più importante. Si tratta, a ben vedere, di un livello di aggressione dell'intimità individuale che sfiora l'inviolabilità della psiche e coinvolge lo statuto della dignità umana, forse priva di espressa menzione nella Carta fondamentale, ma indubitabilmente annoverabile tra i diritti inviolabili della persona.

5.2 Il caso "Bisignani"

La cronaca recente porta alla luce un altro importantissimo caso in cui gli inquirenti hanno fatto uso, per finalità investigative, del c.d. "virus di Stato". Il riferimento è all'indagine sulla presunta associazione di stampo massonico P4. L'indagine fu avviata dalla Procura della Repubblica presso il Tribunale di Napoli. Secondo gli inquirenti, gli imputati avrebbero instaurato, grazie ad un'intricata rete di influenti amicizie, un sistema informativo parallelo che avrebbe avuto tra i suoi obiettivi «...l'illecita acquisizione di notizie e di informazioni, anche coperte da segreto, alcune delle quali inerenti a procedimenti penali in corso nonché di altri dati sensibili o personali al fine di consentire a soggetti inquisiti di eludere le indagini giudiziarie ovvero per ottenere favori o altre utilità».

---

[424] Sul concetto di "prova incostituzionale", si rinvia *supra*, al par. 2.3.1. *Cfr*, inoltre, C. CONTI, *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali*, cit., pp. 485-508. V., *amplius*, C CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007, p. 172. Cfr., inoltre, V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, cit., p. 341.

[425] Cfr. C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, cit., p. 172, nonché P. TONINI - C. CONTI, *Il diritto delle prove penali*, cit., pp. 392 e ss.

In questo caso (svoltosi nel 2007[426]), il captatore informatico era in grado non soltanto di acquisire ed estrapolare dati ed informazioni di natura digitale memorizzati sulla memoria di massa del sistema informatico "bersaglio", ma anche di realizzare una vera e propria intercettazione ambientale, prendendo il controllo occulto del microfono e della webcam dell'elaboratore. I sostituti procuratori incaricati delle indagini si rendono conto immediatamente che nell'utilizzo di siffatto strumento investigativo è necessario contemperare le esigenze investigative finalizzate all'accertamento del fatto con i diritti di difesa delle persone sottoposte ad indagine. Ed infatti, chiedono al g.i.p. di voler autorizzare, con decreto, tanto la *online search*, quanto la *online surveillance*, ai sensi degli art. 266 e ss. c.p.p. Il giudice per le indagini preliminari, investito della questione, ritiene che la prima attività sia perfettamente assimilabile ad una intercettazione ambientale, seppur effettuata attraverso lo strumento atipico della "cimice informatica", e la autorizza con decreto a norma dell'art. 267 c.p.p. Quando alla seconda attività, egli non si discosta dal *decisum* della Cassazione del 2010, ritenendo sufficiente un provvedimento del P.M. a garantire le esigenze di riservatezza dei soggetti interessati[427].

Con riferimento a quest'ultimo aspetto -che riguarda la captazione a distanza di informazioni non aventi carattere comunicativo- valgono le medesime considerazioni critiche svolte infra con riferimento alla sentenza "Virruso". Quanto, invece, all'incasellamento giuridico della *online surveillance* –ossia la captazione di informazioni a contenuto comunicativo- nell'ambito della disciplina propria delle intercettazioni telematiche, occorre fare qualche distinguo.

Quando il flusso comunicativo bidirezionale o pluridirezionale intercettato attraverso il virus consiste in email, messaggi di chat, sms, ecc., *nulla quaestio* circa la copertura giuridica offerta dall'art. 266-*bis* del codice di rito: si tratta, a tutti gli effetti, di una tipologia di intercettazione telematica che trova la sua disciplina tipica negli artt. 267 e ss. c.p.p.[428].

Quando, invece, come nel caso *de quo*, il virus consente di effettuare una vera e propria intercettazione ambientale, la questione si complica in ragione del combinato disposto degli

---

[426] Si tratta del procedimento penale n. 39306/2007 R.G.N.R., mod. 21, incardinato presso la Procura della Repubblica del Tribunale di Napoli.

[427] «Quanto invece all'estrapolazione […] di dati non aventi ad oggetto un flusso bidirezionale (o pluridirezionale) di comunicazioni inteso in senso stretto, ma piuttosto documenti e dati informatici già formati (o che verranno formati in futuro) contenuti nella memoria del personal computer, anche alla luce dell'arresto giurisprudenziale citato dal P.M. e che si richiama, ritiene il giudicante che si tratti di un'attività che esula dalla nozione di intercettazione di comunicazioni o conversazioni. Come tale non deve essere autorizzata dal G.I.P.». Così si legge nel decreto di autorizzazione alle intercettazioni emesso nell'ambito del procedimento in esame.

[428] Cfr., per un approfondimento, S. DE FLAMMINEIS, *Le intercettazioni telematiche*, cit., p. 988.

artt. 266, comma 2, e 614 c.p. Infatti, «l'intercettazione di comunicazioni tra presenti richiede l'indicazione dell'ambiente nel quale l'operazione deve avvenire […] quando si tratti di abitazioni o luoghi privati, secondo l'indicazione di cui all'art. 614 c.p.»[429]. Sennonché, l'utilizzo della "cimice informatica" esclude a priori la possibilità di predeterminare con esattezza i luoghi in cui avverrà l'operazione di intercettazione ambientale. E' noto, infatti, che il personal computer portatile, ma anche e soprattutto lo *smartphone* o il *tablet*, seguono la persona ovunque, in maniera del tutto imprevedibile e non pronosticabile. Ebbene, l'impossibilità di stabilire con esattezza gli spostamenti dello strumento digitale e, quindi, l'inattuabilità della previsione dei luoghi per i quali far autorizzare, da parte del g.i.p., le operazioni di intercettazione svilisce i limiti imposti dalla giurisprudenza di legittimità all'utilizzo delle intercettazioni ambientali[430] e stride con le prerogative di riservatezza sancite a livello costituzionale[431].

5.3 Il caso " Ryanair"

Da ultimo, un recente intervento giurisprudenziale della Suprema Corte[432] ha consentito di ribadire, anche in ambito digitale, un orientamento in realtà già fatto proprio da tempo dalla giurisprudenza di legittimità[433]: i mezzi di ricerca della prova, nessuno escluso, non possono prescindere dalla previa acquisizione di una qualificata notizia di reato, non essendo consentito, nel nostro ordinamento giuridico, utilizzare uno strumento atipico con finalità esplorative di tipo preventivo.

Nel caso de quo, il P.M. aveva disposto il sequestro e la perquisizione delle credenziali di accesso al sistema di *booking online* di una nota compagnia aerea, motivando il provvedimento sulla base dell'esigenza investigativa di identificare in tempo reale i passeggeri sospettabili di fungere da corrieri internazionali di sostanze stupefacenti (c.d. ovulatori)[434].

La Cassazione -nel rigettare il ricorso promosso dalla Procura contro l'ordinanza di annullamento emessa dal Tribunale del Riesame- ha ribadito il divieto di condurre indagini di

---

[429] Così, Cass. pen., sez. VI, 2 dicembre 1999, n. 3541, in *Cass. pen.*, 2000, 3352.
[430] *Ibidem.*
[431] Così, A. TESTAGUZZA, *I sistemi di controllo remoto: fra normativa e prassi*, in *Dir. proc. pen.*, 6, 2014, p. 762.
[432] Cass. pen., Sez. IV, 17 aprile 2012 n. 19618, in *CED* 252689.
[433] Cass. pen. Sez. VI, 17 giugno 1997, n. 2473, in *CED* 209122 e successive conformi.
[434] In base ad una serie di parametri sintomatici desumibili dalle modalità di prenotazione dei voli (soprattutto eseguite *last minute*, in orario notturno, con rientro programmato entro pochissimi giorni dall'arrivo).

tipo esplorativo, non fondate, cioè, sulla esistenza di specifiche notizie di reato: «l'ordinamento processuale colloca i provvedimenti di perquisizione e sequestro tra i mezzi di ricerca della prova, tali provvedimenti presuppongono perciò l'esistenza di una *notitia criminis* e l'avvenuta iscrizione del procedimento nel relativo registro. Coerentemente con tale collocazione, per l'emissione del provvedimento è richiesta la forma del decreto motivato che deve necessariamente contenere l'indicazione della fattispecie concreta nei suoi estremi essenziali di tempo, luogo e azione nonché della norma penale che si intende violata, non essendo sufficiente la mera indicazione del titolo di reato»[435]. Qualora si consentisse diritto di cittadinanza a tale strumento processuale – si è osservato – «si verrebbe […] ad integrare un nuovo ed anomalo strumento di ricerca della prova, con finalità nettamente esplorative, di mera investigazione (paragonabile alle intercettazioni), che nulla ha a che fare con la perquisizione»[436].

6. Uno sguardo oltre i confini nazionali

6.1 La Corte costituzionale tedesca

Sulla questione del c.d. "captatore informatico", si registra una interessantissima sentenza della Corte costituzionale federale tedesca del 27 febbraio 2008[437], con la quale, per la prima volta nel panorama giuridico europeo, viene riconosciuta in capo all'individuo l'esistenza di un nuovo diritto costituzionale: il «diritto fondamentale alla garanzia dell'integrità e della riservatezza dei sistemi informatici», inteso come espressione del più generale «diritto alla dignità» dell'individuo-utente[438].

---

[435] Così, Cass. pen., Sez. IV, 17 aprile 2012 n. 19618, in *Cass. pen.*, 2013, p. 1523 ss.
[436] *Ibidem.*
[437] Si tratta della sentenza del *Bundesverfassungsgericht* del 27 febbraio 2008 sulla c.d. *online durchsuchung*, cit., p.683.
[438] Questo nuovo diritto, secondo i giudici tedeschi, «protegge la vita personale e privata dei titolari dei diritti dall'accesso statale a dispositivi tecnologici di informazione, in particolare dall'accesso da parte dello Stato ai sistemi tecnologici di informazione nel loro complesso, non solo dunque per eventi di comunicazione individuale o memorizzazione dei dati […]. Con la formulazione del nuovo diritto fondamentale alla segretezza ed integrità dei sistemi informatici, la Corte, per la prima volta, ha riconosciuto che le tecnologie non svolgono solo un ruolo importante nella vita delle persone come un'aggiunta o un'estensione al vivere nel mondo fisico, ma anche che un numero crescente di persone vive "in linea". Internet è diventato uno spazio di vita, dove le persone incontrano amici, formano società e scambiano informazioni, e la Corte ha riconosciuto che la normativa esistente non è sufficiente a proteggere adeguatamente i cittadini dalle violazioni da parte dello stato di questo ambiente digitale. Il "cittadino digitale", come risultato di questo caso, ha fatto un passo in avanti». Con una

L'operazione additiva del Giudice delle leggi tedesco nasce dalla dubbia legittimità costituzionale della legge sulla protezione della Costituzione del Nord Reno-Westfalia rispetto agli artt. 10 (segretezza della corrispondenza e delle comunicazioni) e 13 (inviolabilità del domicilio) della Legge fondamentale tedesca (GG).

In particolare, l'art. 5, comma 2, n. 11 della citata legge[439] consentiva ad un organismo di intelligence di derivazione governativa[440] il monitoraggio e l'accesso segreto ai sistemi informatici collegati in rete. Nella pratica, la norma in argomento avrebbe garantito ai servizi segreti del Nord Reno-Westfalia il diritto di cercare ed intercettare in modo occulto comunicazioni via Internet, nonché la possibilità di accedere segretamente a qualsiasi sistema informatico collegato in rete[441].

La Corte costituzionale federale tedesca ha statuito che l'emendamento alla legge, così come formulato, non era conforme a Costituzione. Più che la conclusione (largamente pronosticata), la vera sorpresa è stata il complesso ragionamento argomentativo usato dalla Corte: anziché sfruttare le potenzialità di tutela offerte dai già sperimentati diritti costituzionali esistenti, la declaratoria di incostituzionalità è scaturita dal contrasto tra l'attività di intelligence in argomento (la ricerca a distanza dei dati contenuti su dispositivi digitali) rispetto ad un nuovo diritto fondamentale, che tutela il cittadino digitale nell'uso delle tecnologie di informazione e di comunicazione in rete.

Innanzitutto, la Corte costituzionale tedesca ha precisato che la ricerca a distanza di dati e informazioni memorizzate su sistemi informatici collegati in rete non è equiparabile tout-court ad una intercettazione di comunicazioni. Per tale motivo, nessuna interpretazione analogica dell'art. 10 della legge fondamentale sarebbe in grado di fornire adeguata tutela rispetto a questo nuovo metodo di investigazione[442].

---

precisazione: la ricerca *online* per fini investigativi di repressione del crimine è possibile, ma solo attraverso una normativa conforme al nuovo diritto costituzionale affermato (ponendosi così in linea con la raccomandazione del Consiglio dell'Unione Europea secondo la quale gli Stati membri dovrebbero facilitare la ricerca segreta dei computer dei sospettati per combattere la criminalità informatica). Così, W. ABEL, *La decisione della corte costituzionale tedesca sul diritto alla riservatezza ed integrità dei sistemi tecnologici d'informazione - un rapporto sul caso BVerfGE*, NJW 2008, 822, disponibile su www.jei.it.

[439] Così come modificato, attraverso un emendamento, il 20 dicembre 2006

[440] Si tratta del *Verfassungsschutzbehorde*, un organismo afferente al Ministero dell'Interno (principali servizi segreti della Germania per gli affari internazionali).

[441] Si tratta della *Online Durchsuchung*. Per un approfondimento, si rinvia a R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online* durchsuchung, cit., p. 696.

[442] Art. 10 Costituzione tedesca - 1 La riservatezza della corrispondenza, della posta e delle telecomunicazione è inviolabile. 2. Le restrizioni possono essere ordinate solo in virtù della legge. Se la restrizione serve a proteggere il libero ordine democratico fondamentale o l'esistenza o la sicurezza della Federazione o del Lander, la legge

Nemmeno l'art. 13 della Costituzione tedesca, ad avviso dei giudici, è in grado di fornire sufficiente protezione. Tale disposizione, infatti, tutela la sfera spaziale in cui si estrinseca la vita privata di un individuo contro ogni tipologia di intrusione[443]. Sennonché, la raccolta a distanza di dati sensibili attraverso virus trojan prescinde dal luogo fisico in cui si trova l'individuo, il quale potrebbe benissimo utilizzare dispositivi portatili (personal computer portatili, smathphone, tablet, ecc.) in luoghi pubblici o aperti al pubblico non coperti dalla garanzia costituzionale offerta dall'art. 13[444].

Quindi, dopo aver preso in considerazione ed escluso sia i principi desumibili dall'art. 10, sia quelli derivanti dall'art. 13, perché ritenuti insufficienti, la Corte tedesca ha affermato l'esistenza di un nuovo diritto costituzionalmente garantito alla riservatezza ed alla integrità dei sistemi informatici. Così come il diritto all'autodeterminazione informativa, questo nuovo diritto fondamentale viene ricondotto all'art. 1.1 della Costituzione tedesca, il quale dispone che «la dignità umana è inviolabile e tutti gli organi dello Stato hanno l'obiettivo finale di proteggerla»[445].

Da questa pronuncia emerge come oggi lo sviluppo della personalità dell'individuo non possa prescindere dall'uso della tecnologia informatica e, in particolare, della rete. Internet non è più soltanto uno strumento che consente di accedere ad una quantità illimitata di informazioni, ma è anche e soprattutto un mezzo per stabilire e coltivare i contatti sociali. Inoltre, i dati e le informazioni che gli utenti creano e conservano tramite i propri dispositivi, lungi dall'essere "neutri", hanno ad oggetto il comportamento degli utenti stessi[446]. In buona sostanza, si tratta di dati da cui è possibile ricavare elementi sulla personalità dell'individuo, tracciandone un vero e proprio profilo[447].

---

può prevedere che la persona interessata non debba essere informata della restrizione e che il ricorso ai tribunali venga sostituito da una revisione del caso da parte di agenzie e agenzie ausiliarie nominate dal legislatore.

[443] Art. 13 Costituzione tedesca – 1. La dimora è inviolabile. 2. Le ricerche possono essere autorizzate solo da un giudice o, quando il tempo è essenziale, da altri autorizzati designati dalla legge, e possono essere effettuate solo nei modi in questa prescritti [*omissis*].

[444] «Questo avrebbe comportato la paradossale conseguenza che un cittadino che inizi a scrivere un'email sul suo computer portatile a casa e la riesamini su una panchina del parco completandola e rimandandola a casa si muova tra ambienti protetti e non protetti, perdendo e guadagnando la protezione costituzionale, creando distinzioni artificiali in un'attività percepita da parte del cittadino come uniforme». Così, W. ABEL, *La decisione della corte costituzionale tedesca sul diritto alla riservatezza ed integrità dei sistemi tecnologici d'informazione - un rapporto sul caso BVerfGE*, NJW 2008, 822, cit.

[445] Nel sistema tedesco, questo rappresenta un principio fondamentale di carattere generale progettato per adeguare, in termini garantistici di tutela, le soluzioni legislative al cambiamento sociale.

[446] In effetti, attraverso il monitoraggio della navigazione web, ad esempio, è possibile individuare le attività svolte quotidianamente da ciascuno, le preferenze sessuali o religiose, le situazioni personali, ecc.

[447] Cfr. la sentenza del *Bundesverfassungsgericht* del 27 febbraio 2008 sulla c.d. *online durchsuchung*, cit., p. 683.

Ebbene, la Corte costituzionale tedesca ha affermato che gli utenti godono di una legittima aspettativa di riservatezza rispetto a questi dati, la cui segretezza ed integrità rappresentano diritti fondamentali dell'individuo. Tali diritti devono essere tutelati contro l'accesso segreto, per mezzo del quale possono potenzialmente essere spiati e manipolati tutti i dati disponibili, compresi quelli temporaneamente conservati su supporti di memorizzazione del sistema[448].

Secondo la Corte, il ricorso a nuove forme di investigazione tecnologica non è di per sé contrario a Costituzione. Tuttavia, la loro regolamentazione, a livello legislativo, e la loro utilizzazione, a livello esecutivo, non possono non tener conto del bilanciamento con eventuali interessi contrapposti, a partire dai diritti fondamentali dell'individuo.

Per il legislatore, a livello di tecnica normativa, ciò si traduce nell'obbligo di rispettare i principi di chiarezza e di sufficiente determinatezza della fattispecie, oltre al rispetto del principio di proporzionalità.

Chiarezza e precisione garantiscono al cittadino la piena comprensione della legge, consentendogli di regolare la condotta in modo conforme ai precetti normativi: il legislatore deve determinare in modo chiaro e preciso i casi, le finalità ed i limiti delle eventuali restrizioni dei diritti fondamentali[449]. Una tecnica legislativa basata su meri rinvii ad altre norme - al fine della individuazione dei presupposti che legittimano o meno un determinato comportamento - non rispetta il criterio di sufficiente determinatezza della fattispecie[450].

Proporzionalità, invece, significa che una legge che preveda la compressione di diritti fondamentali deve perseguire uno scopo legittimo e ben individuato e deve essere idonea ed opportuna quale mezzo per il raggiungimento di tale fine. Secondo la Corte, unico scopo che possa giustificare l'accesso ed il monitoraggio segreto su Internet è la necessità di proteggere importanti e predominanti beni giuridici, quali la vita, l'incolumità fisica e la libertà dei singoli, la cui minaccia tocca le fondamenta di uno Stato di diritto[451]. Di conseguenza, nel contesto di un generico obiettivo di prevenzione la compressione di diritti fondamentali non soddisfa il principio di proporzionalità (adeguatezza).

Per questi motivi, nel caso *de quo*, la Corte costituzionale tedesca ha ritenuto il par. 5, comma 2, n. 11 del VSG non conforme ai principi di chiarezza, determinatezza e

---

[448] *Ibidem*.
[449] Cfr. la sentenza del *Bundesverfassungsgericht* del 27 febbraio 2008 sulla c.d. *online durchsuchung*, cit., p. 684.
[450] *Ibidem*: «[…] in quanto la risposta alla questione su quali diritti fondamentali incidano le misure investigative adottate dalla agenzia per la protezione della Costituzione richiede valutazioni complesse, che sono in primo luogo a carico del legislatore, il quale non può esimersi dall'effettuarle limitandosi ad un mero rinvio».
[451] *Ivi*, p. 685.

proporzionalità in senso stretto, dichiarandolo incostituzionale. «La declaratoria di incostituzionalità non riguarda, pertanto, i nuovi mezzi "di carattere tecnologico" in quanto tali ed in termini assoluti, ma (i loro modi di utilizzo) i presupposti ed i limiti, anche temporali, per la loro adozione, secondo i principi che deve seguire il legislatore nel formulare la norma, oltre che la mancata riserva, in ordine alla verifica sulla sussistenza di simili presupposti, ad un organismo indipendente e neutrale. In altre parole il legislatore avrebbe dovuto determinare i casi, le finalità ed i confini della compressione del diritto fondamentale, in modo da rendere chiara e precisa, in termini di formulazione legislativa, la "zona" di intervento -riferita a gravi reati a tutela di importanti beni giuridici- nel rispetto del principio di proporzionalità, nonché prevedere quella riserva all'autorità giudiziaria»[452].

6.2 Qualche timido tentativo legislativo

La non procrastinabilità di una seria e matura riflessione sulla *online surveillance* deriva anche dagli stimoli che provengono dall'Unione Europea. Nelle Conclusioni del Consiglio del 27 novembre 2008, relative ad una strategia di lavoro concertata e a misure pratiche di lotta alla criminalità informatica[453], seppur in un'ottica di contrasto al carattere transnazionale dei reati commessi a mezzo Internet[454], si invitavano espressamente gli Stati membri ad agevolare nel medio termine «la perquisizione a distanza, se prevista nella legislazione nazionale, che consente ai servizi investigativi di accedere rapidamente alle informazioni, con l'accordo del paese ospite»[455]. Nel quadro delle accresciute competenze penali attribuite all'Unione dal Trattato di Lisbona[456], va poi ricordata la direttiva del 2011 sulla lotta alla pedopornografia[457], che al *considerandum* 27 auspica come «strumenti investigativi efficaci dovrebbero essere messi a disposizione dei responsabili delle indagini e dell'azione penale relative ai reati di cui alla presente direttiva. Tali strumenti potrebbero includere l'intercettazione di comunicazioni, controlli a distanza anche con uso di strumenti elettronici di sorveglianza, il controllo dei

---

[452] Così, R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online* durchsuchung, cit., pp. 709 ss.
[453] Pubblicate in G.U.U.E. 17 marzo 2009, C 62/16.
[454] D'altronde, le c.d. *remote computer searches* consentono di avere accesso a computers ovunque essi siano localizzati, quindi anche al di fuori dei naturali confini della giurisdizione di uno Stato. Di qui la necessità di un approccio globale al fenomeno.
[455] «Tale disposizione sembra […] fare indiretto riferimento all'istituto delle perquisizioni *on line* (*remote computer searches*)». Così, F. IOVENE, *Le c.d. perquisizioni on line tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Riv. trim. diritto penale contemporaneo*, 3-4, 2014, p. 332.
[456] Tra cui rientra la criminalità informatica (art. 83 TFUE).
[457] Direttiva 2011/93/UE, che sostituisce la DQ 2004/68/GAI, G.U.U.E. 17 dicembre 2011, L 351/1.

conti bancari o altre indagini finanziarie, tenuto conto, tra l'altro, del principio di proporzionalità e del carattere e della gravità dei reati oggetto d'indagine. Se del caso, e conformemente alla legislazione nazionale, tali strumenti dovrebbero comprendere anche la possibilità per le autorità di polizia di usare su Internet nomi di copertura». Anche in questo caso il riferimento sembra essere, tra le altre cose, alle *online searches*[458]. Inoltre, merita di essere citata la proposta di Regolamento per l'istituzione della Procura Europea che, all'art. 26, contiene un elenco di strumenti di indagine che gli Stati membri devono mettere a disposizione del Pubblico Ministero Europeo, con obbligo per questi ultimi di introdurli nell'ordinamento interno se non previsti[459]. Nell'aprile del 2014, infine, è stata approvata la Direttiva relativa all'Ordine Europeo di Indagine Penale[460]: tale strumento, basato sul principio del mutuo riconoscimento, consente all'autorità competente di uno Stato membro di ottenere che l'autorità competente di altro Stato membro compia uno o più atti di indagine specifici e si presta a ricomprendere anche le misure di electronic surveillance.

In definitiva, per quanto riguarda gli strumenti di indagine l'Unione Europea si sta facendo promotrice di un tentativo di rinnovamento e di armonizzazione dei sistemi processuali nazionali. Tuttavia, tale livello di armonizzazione varia in ragione del tipo di mezzo di ricerca della prova[461] e per quanto riguarda le misure di *surveillance*, cui appartengono anche le *online searches*, «l'unico elemento che pare accomunare le legislazioni nazionali è l'assenza di una disciplina puntuale nelle legislazioni nazionali[462]». In questo particolare ambito, infatti, le risposte degli ordinamenti sono state diverse: alcuni hanno reagito, con non pochi problemi di tenuta costituzionale, tipizzando (Germania), o tentando di tipizzare (Olanda e Spagna) i nuovi strumenti investigativi attraverso una disciplina ad hoc; altri sono ricorsi all'applicazione analogica di norme dettate per misure affini o alla categoria della prova atipica (Italia, insieme a tutti gli altri). Il fenomeno non è nuovo, ma sviluppa criticità

---

458 Così, F. IOVENE, *Le c.d. perquisizioni on line*, cit., pp. 332 e 333.

459 Cfr. S. ALLEGREZZA, *Verso una Procura europea per tutelare gli interessi finanziari dell'Unione. Idee di ieri, chances di oggi, prospettive di domani*, in www.penalecontemporaneo.it, 31 ottobre 2013.

460 Direttiva 2014/41/UE, in G.U.U.E. 1 maggio 2014, L 130/1.

461 Come emerso dai lavori preparatori delle *Model Rules* elaborate dall'Università del Lussemburgo per l'istituendo Pubblico Ministero Europeo Il progetto è stato coordinato dalla Professoressa Katalin Ligeti dell'Università del Lussemburgo. Le *Model Rules* e la Relazione introduttiva della Prof. Katalin Ligeti sono disponibili all'indirizzo http://www.eppo-project.eu/index.php/EU-model-rules e saranno pubblicate insieme al report finale in K. Ligeti (ed.), *Toward a Prosecutor for the European Union. Draft Rules of procedure*, Volume 2, Oxford, 2013 (in corso di pubblicazione).

462 S. ALLEGREZZA, *Le misure coercitive nelle «Model Rules for the Procedure of the European Public Prosecutor's Office»*, in F. RUGGIERI, T. RAFARACI, G. DI PAOLO, S. MARCOLINI, R. BELFIORE (a cura di), *Processo penale, lingua e Unione Europea*, Padova, 2013, p. 151 ss.

sconosciute in un contesto in cui sempre più spesso si hanno occasioni di confronto tra sistemi giuridici diversi a causa della transnazionalità della criminalità e della natura digitale della prova[463].

Al di là dell'esperienza tedesca, dove, seppur edulcorata dalla Corte costituzionale, una normativa *ad hoc* esiste sin dal 2006 e dove da tempo dottrina e giurisprudenza si interrogano sui delicati rapporti tra *online durchsuchung* e diritti costituzionalmente garantiti, in tempi recenti, anche nei Paesi Bassi è stata proposta l'introduzione del c.d. "*trojan* di Stato". Rimasto solo un timido tentativo di riforma, tale istituto avrebbe consentito alla polizia, su autorizzazione del giudice, di monitorare l'uso dei sistemi informatici, copiarne i dati e addirittura distruggerli, se illegali[464].

In Spagna, la proposta di autorizzare l'utilizzo per fini investigativi del captatore informatico risale al febbraio 2013[465]: in particolare, attraverso una modifica degli artt. 350, 351, 352 del *Codigo Procesal Penal* si prevedeva la possibilità di installare da remoto uno specifico software di indagine in grado di accedere in modo occulto ai dati contenuti in un sistema informatico[466]. La proposta di legge prevedeva, ovviamente, anche delle garanzie: indicazione tassativa dei reati per i quali era possibile ricorrere al captatore[467]; riserva di giurisdizione[468]; durata massima della intrusione[469]; standard probatorio per attivare l'intrusione informatica[470]; modalità esecutive[471]. Così come in Olanda, anche in Spagna si prevedeva l'eventualità del ricorso ai meccanismi di cooperazione giudiziaria nell'ipotesi in cui il sistema informatico non si fosse trovato nel territorio spagnolo.

Spostando lo sguardo oltre oceano, le soluzioni cambiano: negli U.S.A. esiste un software in grado di captare tutto ciò che viene digitato dall'utilizzatore di un personal computer sulla propria tastiera[472]. Attraverso questo programma gli investigatori sono in grado di accedere al

---

[463] *Ibidem*.
[464] Lo riporta F. IOVENE, *Le c.d. perquisizioni on line*, cit., pp. 329 e ss., la quale sottolinea che la proposta proviene dal Ministro della Giustizia olandese Ivo Opstelten e risale all'ottobre del 2012.
[465] Si deve al Ministro della giustizia spagnolo, Alberto Ruiz Gallardón.
[466] Si parlava di *registros remotos sobre equipos informaticos.*
[467] Reati di particolare gravità.
[468] Il monitoraggio doveva essere autorizzato dal *Tribunal de Garantías*.
[469] Dieci giorni.
[470] La misura doveva essere necessaria e proporzionata per l'accertamento del reato.
[471] La proposta si preoccupava altresì di specificare quale doveva essere il contenuto del provvedimento giurisdizionale, ossia, oltre alla motivazione in ordine alla idoneità, necessità e proporzionalità della misura, anche l'indicazione dello specifico dispositivo oggetto d'indagine, dei dati ricercati, dei soggetti autorizzati a condurre l'indagine e l'eventuale autorizzazione ad effettuare copie, con misure idonee a garantirne l'integrità, dei dati rilevanti.
[472] Si tratta del *keylogger "Magic Lantern"*.

contenuto di cartelle e file, anche se protetti da password. Ebbene, la legittimità di tale strumento di indagine dipende dall'intensità della violazione del bene in giuridico in gioco, ossia la riservatezza dei dati personali criptati e spiati: se esiste una *reasonable expectation of privacy* rispetto ai dati e alle informazioni occultamente captate, è necessario disporre di un mandato, basato su un fondato motivo, in applicazione della c.d. *Fourth Amendment Doctrine*[473]. Viceversa, laddove tale legittima aspettativa manchi, l'utilizzo per fini investigativi di tale strumento invasivo è lasciato alla discrezionalità degli operatori.

7. Considerazioni conclusive

Chi scrive è convinto dell'utilità pratica che riveste il captatore informatico nell'ambito delle investigazioni di natura digitale. D'altronde, il progresso tecnico-scientifico e, purtroppo, il suo utilizzo per fini illeciti esigono una adeguata risposta da parte degli inquirenti che, per rimanere al passo con i tempi, devono agire con strumenti idonei al mutato contesto sociale. In questo settore è particolarmente sentita l'esigenza di una sinergia tra informatica e diritto: compito del diritto è quello di aggiornare, attraverso l'evoluzione legislativa e giurisprudenziale, le tradizionali categorie concettuali in modo da non lasciare i singoli sprovvisti di tutela.

A fronte della ineluttabile esigenza della prassi di ricorrere, sempre più frequentemente, all'uso di strumenti di indagine ad alto contenuto tecnologico, si possono ipotizzare le seguenti, alternative, risposte dell'ordinamento: 1) silenzio-inerzia del legislatore e contestuale supplenza pretoria, sia favorevole che contraria all'utilizzo dello strumento; 2) intervento normativo in chiave preventiva o repressiva.

La prima soluzione è tutt'altro che originale nel nostro sistema. Due esempi su tutti: l'acquisizione dei tabulati di traffico telefonico, prima dell'entrata in vigore del codice della privacy; il tema delle videoriprese, ancora oggi disciplinato dal diritto vivente. D'altronde, l'indagine comparativa dimostra che non ci sono scelte uniformi nei vari ordinamenti e che nella maggior parte dei casi si assiste ad una mancanza di legislazione[474].

---

[473] Cfr. S. W. BRENNER, *Fourth Amendment Future: Remote Computer Searchesand the Use of Virtual Force*, in *81 Miss. L. J.*,1, 2011, che dà atto di come le Corti riconoscano generalmente una legittima aspettativa di privacy rispetto al contenuto dell'hard disk del computer.

[474] Secondo S. ALLEGREZZA, *Le misure coercitive nelle "Model Rules for the Procedure of European Public Prosecutor's Office"*, cit., p. 151, nei lavori preparatori delle Model Rules elaborate dall'Università del

La seconda soluzione merita accoglimento: le innovazioni tecnologiche sono uno strumento importante per la lotta alla criminalità, uno strumento che tuttavia appare essere particolarmente invasivo dei diritti fondamentali della persona; pur nel rispetto del loro nucleo essenziale, tali diritti sono limitabili in un'ottica di bilanciamento con le altrettanto fondamentali esigenze di contrasto alla criminalità. Ebbene, lo scrivente è persuaso che, in un processo penale di stampo accusatorio, lontano da quella onnivora fame di conoscenza che caratterizzava il precedente sistema inquisitorio e che purtroppo a volte riemerge in talune pronunce della giurisprudenza, il bilanciamento tra tutela dei diritti fondamentali ed esigenze investigative di accertamento del fatto criminoso deve essere realizzato dal legislatore, quale autentico interprete del rapporto, difficile ma non per questo procrastinabile, tra tutela individuale e difesa sociale. D'altronde anche a livello europeo l'art. 15, par. 2, della Convenzione di Budapest invita espressamente i legislatori nazionali a disciplinare le indagini informatiche, prevedendo la supervisione di un organo giudiziario indipendente, la limitazione dell'ambito applicativo, l'indicazione della durata delle indagini medesime e la relativa procedura di svolgimento.

Quella del bilanciamento è una metafora tranquillizzante che, tuttavia, rischia di rappresentare solamente una comoda via di fuga teorica senza ulteriori precisazioni. Troppo facile, infatti, sostenere la soluzione dal punto di vista astratto e generico: realizzare un giusto equilibrio tra esigenze di repressione e diritti fondamentali significa trovare il punto mediano in cui i due piatti della bilancia stanno sullo stesso livello. Ma in concreto, dovendo intervenire, come si ottiene tale bilanciamento? Probabilmente si può e si deve sostituire la parola "bilanciamento" con la parola "eccezione": la limitazione ai diritti fondamentali deve rappresentare l'eccezione a favore di comprovate e rilevanti esigenze di prevenzione e di repressione dei reati. La caratteristica fondamentale del principio di proporzionalità è la stretta necessità: ciò significa che le limitazioni dei diritti fondamentali devono essere assolutamente eccezionali, limitate alle singole situazioni concrete e alle singole emergenze. Il pericolo maggiore non è rinunciare al singolo diritto fondamentale in una singola situazione eccezionale e temporanea, ma dimenticarsi del diritto fondamentale. Compito del bilanciamento proporzionale è quello di evitare che ciò avvenga.

Lussemburgo per l'istituendo Pubblico Ministero Europeo emerge come, per quanto riguarda le misure di *surveillance*, nel cui ambito rientrano anche le *on line searches*, «l'unico elemento che pare accomunare le legislazioni nazionali è l'assenza di una disciplina puntuale».

In questo quadro è evidente che l'aggiornamento normativo dovrebbe essere tecnologicamente neutro, perché le riforme legislative non possono stare al passo con l'evoluzione tecnologica. Il rischio, evidente, è che normative troppo di dettaglio sfocino in una facile quanto scontata obsolescenza.

7.1 *De iure condito*

Nel nostro Paese, il primo tentativo di tipizzazione del captatore informatico è piuttosto recente: esso si registra durante i lavori parlamentari svolti in occasione della conversione in legge del decreto-legge 18 febbraio 2015, n. 7, recante «misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione» (c.d. "decreto legge antiterrorismo").

In realtà, nel testo originario del disegno di legge di conversione non veniva fatto alcun accenno al c.d. captatore informatico. L'iniziativa governativa presso la Camera dei Deputati, infatti, non aveva previsto alcunché in proposito. Il tentativo di innovare in tale direzione derivava dal testo proposto dalle Commissioni, il quale, all'art. 2, comma 1-*ter*, esplicitamente prevedeva che «al codice di procedura penale sono apportate le seguenti modificazioni: a) all'art. 266-*bis*, comma 1 ("1. Nei 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 relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi" sono aggiunte le seguenti parole: ", anche attraverso l'impiego di strumenti e di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico"».

Usando un linguaggio penalistico, potremmo dire che l'agire delle Commissioni è rimasto alla soglia del tentativo, tant'è che il testo poi approvato e convertito in legge non contiene alcun riferimento al captatore informatico. Ciò, probabilmente, a causa della impressionante bufera politica che tale tentativo ha sollevato nelle opposizioni.

Al di là delle pur legittime critiche politiche, dal colore vivace ma spesso sfumato, il tentativo di tipizzazione appena visto si espone a riserve insuperabili anche e soprattutto dal punto vista squisitamente giuridico. Innanzitutto, si trattava di una norma che in quanto

genericamente formulata non soddisfaceva in alcun modo quelle esigenze di tassatività proprie di una materia, quella delle intercettazioni, che rappresenta l'implementazione di una riserva di legge rinforzata prevista a livello costituzionale: la previsione dei "casi" e dei "modi" non può certo ritenersi soddisfatta con una norma, come quella in argomento, sintetica e "cerchiobottista". Qualora fosse entrata in vigore, probabilmente sarebbe stata dichiarata incostituzionale, in quanto totalmente priva di proporzione: l'art. 266-*bis* c.p.p., infatti, non prevede i casi (tipi di reato) per i quali è possibile ricorrere ad intercettazione e quindi mal si adatta alle perquisizioni *online*, che, come spiegato, sono qualcosa di molto più invasivo delle intercettazioni stesse. Ma c'è di più: la norma apparsa nel testo delle Commissioni alla Camera non distingueva correttamente tra *online surveillance* e *online search*. In realtà, solo la prima delle due attività (l'acquisizione da remoto delle comunicazioni) può essere ricondotta sistematicamente nell'ambito delle intercettazioni telematiche, mentre per l'altra (l'acquisizione da remoto dei dati presenti in un sistema informatico) la collocazione più corretta sarebbe stata nel capo II o, al limite, nel capo III del Libro III, rispettivamente dedicati a perquisizioni e sequestri.

L'introduzione di una norma di questo tipo sarebbe stato un errore grave da parte del legislatore. Tuttavia, altrettanto grave è l'errore in cui si può incorrere e in cui il legislatore sta continuando ad incorrere, e cioè il silenzio, il non occuparsi di questa realtà. Quando la realtà è sgradevole, non esiste errore più grande dell'ignorarla, perché la realtà si impone. E' inevitabile infatti che di fronte a gravi forme di criminalità, gli organi inquirenti, pressati dal loro ruolo istituzionale, si avvalgano nella prassi di queste tecniche di indagine. Mancandone una disciplina, aumenta il rischio che l'utilizzo che se ne fa risulti distorto e sproporzionato. Questo è l'effetto del vuoto legislativo.

Sempre in una prospettiva *de iure condito*, appare doveroso far cenno alla c.d. "Carta dei diritti di Internet"[475], un decalogo di principi relativi al diritto di accesso alla rete, alla *net neutrality* e, per quanto più di nostro interesse, al delicato rapporto fra diritto alla privacy ed esigenze di giustizia. Ovviamente, la Carta non ha alcun valore vincolante, non si tratta infatti né di una legge, né di una proposta di legge, ma soltanto di *soft law*. Tuttavia, l'obiettivo è chiaro: il testo è da leggere come «un cantiere in evoluzione» su cui la commissione [Commissione di studio sui diritti e i doveri relativi ad Internet, istituita il 28 luglio 2014] «continuerà a lavorare» con l'obiettivo di giungere ad una «mozione unitaria che impegni il

[475] Approvata dalla Camera dei Deputati in data 28 luglio 2015.

governo a promuoverne i contenuti in contesti nazionali e internazionali»[476]. In particolare, è interessante l'art. 7 della Carta (Diritto all'inviolabilità dei sistemi, dei dispositivi e domicili informatici) che precisa il "rango" del bene giuridico coinvolto in ipotesi di compressione del c.d. "domicilio informatico", prevedendo la tutela della doppia riserva, di legge e di giurisdizione.

Nonostante si tratti, per ora, di una sorta di dichiarazione di intenti, ritengo che tale documento sia una chiara dimostrazione della accresciuta sensibilità del nostro Parlamento nei confronti del bene giuridico "riservatezza informatica", con tutte le conseguenze del caso in termini di interpretazione delle norme ad oggi vigenti.

7.2 *De iure condendo*

In una prospettiva *de iure condendo*, le soluzioni prospettabili sono sostanzialmente due: una muove da una logica di prevenzione, l'altra ha una *ratio* repressiva.

Attribuire alle perquisizioni *online* un ruolo di strumento di prevenzione significa individuarne la sede di tipizzazione nelle disposizioni di attuazione del codice di rito, così come avviene oggi per le intercettazioni preventive previste dall'art. 226 disp. att.[477]. Coerentemente con tale scelta, la disciplina dovrebbe essere simile a quella prevista per queste ultime, così come modificata dall'art. 5, comma 1, del d.l. 18 ottobre 2001, n. 374, convertito nella legge 15 dicembre 2001, n. 438. In particolare, la richiesta di autorizzare captazioni preventive dovrebbe spettare ad organi dell'esecutivo: Ministero dell'interno e, su sua delega, questore e comandanti provinciali dei Carabinieri e della Guardia di Finanza[478], ma anche Presidente del Consiglio dei Ministri, con facoltà di delega ai direttori delle Agenzie facenti capo al Sistema di informazione per la sicurezza della Repubblica[479]. L'autorizzazione dovrebbe essere di competenza del Procuratore della Repubblica presso il tribunale del distretto in cui si trova il soggetto da sottoporre a controllo o, nell'ipotesi in cui questi non sia

---

[476] Così, L. BOLDRINI, Presidente della Camera dei Deputati.

[477] Su tale strumento di prevenzione, fra i tanti cfr. C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, cit., pp. 56 e ss, nonché, G. GARUTI, *Le intercettazioni preventive nella lotta al terrorismo internazionale*, in *Dir. pen. proc.*, 2005, p. 1457.

[478] Cfr. art. 12 del d.l. 13 maggio 1991, n. 152, convertito, con modificazioni, nella legge 12 luglio 1991, n. 203.

[479] La legge 3 agosto 2007 n. 124, ha modificato drasticamente la struttura dell'intelligence italiana, in quanto rispetto alla legge del 1977, che in precedenza regolava la materia, divide le competenze non tra strutture approssimativamente distinguibili in civili e militari (ossia SISDE e SISMI), bensì per sfere territoriali di competenza: esclusivamente sul territorio nazionale l'AISI ed esclusivamente all'estero l'AISE, allineando l'Italia ai principali uffici internazionali.

localizzabile, del distretto in cui sono emerse le esigenze di prevenzione. Le operazioni autorizzate dovrebbero consistere nel monitoraggio e nell'acquisizione a distanza dei dati digitali immagazzinati sui dispositivi in uso ai soggetti per i quali si rende necessaria l'attività preventiva. Ovviamente, tale attività di intelligence dovrebbe essere giustificata solo per la prevenzione di delitti di grave allarme sociale e di criminalità organizzata, rispettivamente elencati negli artt. 407, comma 2, lett. a) e 51, comma 3-*bis*, c.p.p. Lo standard probatorio utile ai fini di una corretta motivazione del provvedimento autorizzativo dell'autorità giudiziaria non sembrerebbe comunque poter fare a meno di sufficienti elementi investigativi che consentano di qualificare come "necessaria", in concreto, l'attività di prevenzione. Ultimo, ma non certo per importanza, aspetto da considerare è quello relativo ai risultati di tali invasivi strumenti di prevenzione, i quali non dovrebbero mai avere valenza probatoria, ma solo funzione investigativa (orientare le indagini).

Sennonché, fare delle perquisizioni *online* uno strumento di pubblica sicurezza volto a impedire, in una prospettiva *ex ante*, la perpetrazione di illeciti penali non sembra essere la soluzione migliore per risolvere il problema del vuoto di disciplina positiva che attualmente esiste con riferimento a questo tipo di strumento investigativo. Ed infatti, si ripresenterebbero anche per le perquisizioni *online* gli stessi dubbi, peraltro mai sopiti, di legittimità costituzionale che caratterizzano le intercettazioni e i controlli preventivi sulle comunicazioni di cui all'art. 226-*bis* disp. att. c.p.p.[480]. Inoltre, nell'ambito di un eventuale processo penale avviato all'esito di tali invasive attività diventerebbe difficile nella prassi applicativa escludere l'effettivo utilizzo delle informazioni acquisite per fini di prevenzione[481].

Per questi motivi, l'opzione più convincente, sempre in una prospettiva *de iure condendo*, sembra essere quella di inserire le perquisizioni *online* tra i mezzi di ricerca della prova, con una funzione repressiva, dunque, di reati già commessi o il cui *iter criminis* sia in corso di svolgimento.

---

[480] Cfr. C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p. 56, nota 142, dove l'a. riassume i seguenti profili di potenziale incostituzionalità delle c.d. intercettazioni preventive: «la mancata previsione nella Carta fondamentale delle esigenze preventive fra i valori la cui tutela consenta la compressione della libertà e della segretezza delle comunicazioni; l'asserita violazione della riserva di giurisdizione, di cui all'art. 15 comma 2 Cost. […]; il difetto di tassatività dei presupposti applicativi e la mancata previsione di un limite temporale per l'esecuzione delle misure».

[481] Con riferimento alle intercettazioni preventive, cfr. Cass., sez. V, 1 febbraio 2001, Di Zeno, in *CED Cass.*, n. 217938; Cass., sez. V, 27 settembre 2000, Brunella, *ivi*, n. 217978.

Una ipotetica regolamentazione dovrebbe contenere i seguenti elementi indefettibili: 1) tipologie di reati per i quali è ammissibile il ricorso allo strumento investigativo[482]: 2) standard probatorio che deve essere soddisfatto per innescare il potere investigativo[483]; 3) *target*, ossia obiettivo della intrusione investigativa[484]; 4) tecniche di intrusione, ossia modalità di espletamento dello strumento investigativo[485].

Sulla base di tali criteri, si tenterà a questo punto di proporre una possibile opzione di modifica dell'attuale codice di rito, proponendo la tipizzazione di un nuovo mezzo di ricerca della prova, il c.d. "captatore informatico".

[482] Quando parliamo di indagini informatiche è opportuno innanzitutto un chiaro riferimento al tipo di reato, che deve essere di particolare gravità.

[483] Gravità indiziaria o sufficienti indizi? Di reato o di reità? E' necessario, inoltre, porsi il problema relativo all'origine delle informazioni che vengono utilizzate per soddisfare tale soglia (ad esempio, è ammissibile l'utilizzo a tali fini dei risultati dell'attività di intelligence? A quali condizioni?)

[484] L'obiettivo deve essere il più possibile precisato, perché una cosa è sottoporre a monitoraggio il dispositivo in uso all'indagato, ben altra cosa è controllare i dispositivi digitale di terzi: si deve spiegare qual è il collegamento tra il terzo, apparentemente estraneo al reato, e la fattispecie di reato per cui si procede.

[485] Tecnicamente, si devono utilizzare metodi di indagine che non annullino il diritto fondamentale coinvolto nell'accertamento, minimizzando l'intrusione e garantendo, altresì, la genuinità e la conservazione delle informazioni acquisite.

Allegato – Proposta di inserimento, nel codice di procedura penale, Libro III, Titolo III, del capo V (artt. 271-*bis* – 271-sexies)

Capo V

Programmi informatici per l'acquisizione da remoto dei dati e delle informazioni presenti in un sistema informatico o telematico

Art. 271-*bis*. Limiti di ammissibilità.

1. La captazione di dati o di informazioni digitali di qualsiasi natura è consentita esclusivamente nei procedimenti relativi ai delitti indicati negli articoli 407, comma 2, lett. a) e 51, comma 3-*bis*.

2. Per captazione si intende la copia totale o parziale, da remoto, del contenuto informativo di un dispositivo digitale di memorizzazione collegato in rete, ovvero il monitoraggio, da remoto, delle operazioni svolte attraverso un sistema informatico o telematico connesso alla rete Internet.

Art. 271-*ter*. Presupposti e forme del provvedimento.

1. Il pubblico ministero richiede al giudice per le indagini preliminari l'autorizzazione a disporre le operazioni previste dal comma 2 dell'art. 271-*bis*. L'autorizzazione è data con decreto motivato quando vi sono gravi indizi di reato e la captazione è assolutamente indispensabile ai fini della prosecuzione delle indagini.

2. Nella valutazione dei gravi indizi di reato si applicano le disposizioni degli articoli 192, commi 2, 3 e 4, 195, comma 7, 203 e 201, comma 1.

3. Nei casi di urgenza, quando sussistono specifiche ed inderogabili esigenze attinenti alle indagini relative ai fatti per i quali si procede, in relazione a situazioni di concreto ed attuale pericolo per l'acquisizione o la genuinità della prova, il pubblico ministero dispone la captazione con decreto motivato, che va comunicato immediatamente e comunque non oltre le ventiquattro ore al giudice indicato nel comma 1. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non viene convalidato nel termine stabilito, la captazione non può essere proseguita e i risultati di essa non possono essere utilizzati.

4. Il pubblico ministero dispone con decreto le modalità e la durata delle operazioni di captazione, che non può superare i quindici giorni, ma può essere prorogata dal giudice con

decreto motivato, su richiesta del pubblico ministero, per periodi successivi di quindici giorni, qualora permangano i presupposti indicati nel comma 1.

5. Alle operazioni di captazione procede il pubblico ministero, personalmente o delegando ufficiali di polizia giudiziaria, i quali si possono avvalere dell'ausilio di uno o più agenti di polizia giudiziaria.

6. In apposito registro riservato tenuto nell'ufficio del pubblico ministero sono annotati, secondo un ordine cronologico, i decreti che autorizzano, dispongono e prorogano le operazioni di captazione e, per ciascuna captazione, l'inizio e il termine delle operazioni.

271-*quater*. Esecuzione delle operazioni

1. Le informazioni captate sono memorizzate su un adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. Delle operazioni è sempre redatto verbale.

2. Le operazioni possono essere compiute, alternativamente o cumulativamente, per mezzo degli impianti installati nella procura della Repubblica, mediante impianti di pubblico servizio o in dotazione alla polizia giudiziaria, ovvero mediante impianti appartenenti a privati.

3. Si applicano le disposizioni contenute nei commi 4, 5, 6, 7 e 8 dell'art. 268, salvo incompatibilità.

271-*quinquies*. Conservazione delle informazioni

1. I verbali e i supporti contenenti le informazioni captate sono custoditi, in apposito archivio riservato, presso l'ufficio del pubblico ministero che ha disposto le operazioni, ovvero in altro luogo idoneo a preservare la genuinità e la immodificabilità dei risultati acquisiti, individuato con decreto motivato del pubblico ministero.

2. Si applicano le disposizioni contenute nei commi 2 e 3 dell'art. 269, salvo incompatibilità.

271-sexies. Divieti di utilizzazione

1. I risultati delle operazioni di captazione non possono essere utilizzati qualora le stesse siano state eseguite fuori dei casi consentiti dalla legge o qualora non siano state osservate le disposizioni previste dal presente capo.

2. Si applicano, in quanto compatibili, le disposizioni contenute negli articoli 270, 270-*bis* e 271, commi 2 e 3.

CAPITOLO 4
LE INTERCETTAZIONI TELEMATICHE

Sommario: 1. Le intercettazioni di comunicazioni telematiche - 2. Virus informatico, intercettazioni ambientali e videoriprese - 2.1 Sulle intercettazioni ambientali tramite virus informatico - 2.2 Sulle videoriprese

1. Le intercettazioni di comunicazioni telematiche

Le c.d. intercettazioni telematiche, come mezzi di ricerca della prova tipici e autonomi rispetto alle intercettazioni tradizionali[486], sono state introdotte nel codice di rito dagli artt. 11[487] e 12[488] della legge 23 dicembre 1993, n. 547[489]. Oggetto di intercettazione telematica possono essere tutte le comunicazioni realizzate tramite sistemi informatici o telematici, ossia tra computer collegati tra loro in rete, via modem, via radio (se i dispositivi sono connessi con tecnologia wireless) o con qualsiasi altra forma di interconnessione[490].

Da un punto di vista squisitamente tecnico, l'intercettazione telematica consiste nell'acquisizione di pacchetti di dati in transito sulla rete. Da un punto di vista empirico, tali

---

[486] All'indomani della emanazione della l. 547 del 1993, alcuni commentatori contestarono l'utilità pratica della disposizione contenuta nell'art. 266 *bis* c.p.p. 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.), sì 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. 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. Così, G. FUMU, *sub art. 266 bis* in *Commento al codice di procedura penale*, coordinato da M. CHIAVARIO, III agg., Torino 1998.

[487] Che ha introdotto l'art. 266-*bis* c.p.p. (Intercettazioni di comunicazioni informatiche o telematiche.): «Nei 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 relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi».

[488] Che ha previsto l'art. 268, co. 3-*bis* c.p.p., secondo il 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».

[489] Pubblicata nella G.U. 30 dicembre 1993, n. 305.

[490] Sempre tecnicamente, esistono diversi livelli di intercettazione digitale in quanto la rete opera in maniera stratificata, ossia impiega layer che sono il più possibile impermeabili tra loro per ragioni di convenienza economica e tecnica. Attraversando i diversi livelli si può avere quindi: 1) intercettazione su cavo del segnale di basso livello e ricostruzione completa dei protocolli; 2) intercettazione presso il Provider di servizi Internet, ossia l'ente privato o pubblico che permette la particolare connessione (spesso gli Internet Service Provider = ISP); 3) intercettazione sulle dorsali (*backbone*) di comunicazione con separazione e filtraggio dei dati. Cfr. M. MATTIUCCI, *Intercettazioni digitali*, www.marcomattiucci.it, 30 novembre 2015.

intercettazioni consistono nel complesso di attività ed operazioni dirette a captare comunicazioni e/o conversazioni che avvengono attraverso strumenti informatici e/o telematici. La comunicazione informatica tra due o più soggetti può avvenire tramite il tradizionale scambio di email o per mezzo delle più svariate applicazioni che consentono l'interazione in tempo reale o differito (servizi di messaggistica e di chat[491]). La conversazione vocale, invece, avviene attraverso la c.d. tecnologia Voip[492], che sta letteralmente rivoluzionando il mondo della telefonia. Ebbene, le concrete modalità operative di esecuzione delle intercettazioni telematiche ed informatiche sono fortemente condizionate

[491] Twitter, WhatsApp, Wechat, ecc., tutti facilmente disponibili e scaricabili dalla rete e generalmente ottimizzati per un uso su apparati mobili come gli smartphone, sia nelle piattaforme Android (Samsung ed altri) che IOS (Iphone ed Ipad). Lo scenario che si presenta, almeno per quanto riguarda la parte intercettiva dei canali di comunicazione, è assai complicato, sia per la varietà di sistemi ed applicazioni utilizzate, sia per la possibilità di connettersi praticamente ovunque con linee di collegamento sempre diverse (Wifi aperti, schede UMTS, adsl domestiche, ecc.), con apprezzabili margini di sicurezza per comunicare senza essere individuati e intercettati. E' recentissima la triste cronaca dei fatti di Parigi, dove secondo alcune fonti non confermate l'attacco terroristico del 13 novembre 2015 sarebbe stato preparato usando una console PS4 e la chat del PlayStation Network. Tutto è nato dall'interpretazione di un intervista rilasciata dal ministro belga Jan Jambon e dal fatto che sia stata ritrovata una console in uno dei covi usati dai terroristi. La consolle permette infatti di parlarsi o chattare in modalità criptata, come su Skype. «Nel caso della PlayStation, i metodi di interazione tra utenti sono molteplici e "intercettarli" tutti al momento si tradurrebbe in un compito complesso. Nel caso più semplice, due o più persone possono comunicare sul PlayStation Network attraverso semplici messaggi di testo, che previa disponibilità all'accesso da parte di Sony (l'azienda che produce il sistema e gestisce il relativo "cloud") sotto le mani degli investigatori, possono anche venire captati con relativa semplicità. Ma naturalmente il giorno dopo l'apertura a controlli più severi, non li utilizzerebbe più nessuno per comunicazioni da tenere nascoste. Diverso e infinitamente più frastagliato è il caso delle comunicazioni "in-game", quelle che avvengono all'interno dei giochi *online*, dove più giocatori si riuniscono e possono comunicare per scritto ma anche - e soprattutto - a voce e in video, privatamente e pubblicamente, verbalmente o con linguaggi visuali. In eventi-partite collettive non necessariamente aperte al pubblico ma destinate a utenti selezionati. Perché il digitale può abbattere le barriere ma anche essere usato per crearne di nuove. Intercettare quelle comunicazioni significa di fatto doversi "infiltrare" all'interno di comunità *online* sospette per svolgere un lavoro di intelligence del tutto simile a quello dei servizi sul territorio. Ma qui il panorama di possibili incroci giochi-orari-partite-server proprietari (le infrastrutture dei giochi *online* non passano tutte da Sony) potrebbe rivelarsi un terreno improbo, a meno di non prevedere una sorta di filtro a monte e sofisticate tecnologie di rilevazione di contenuti e meeting sospetti. Che richiederebbe qualcosa di simile a delle "leggi speciali" per i giochi *online*, che al momento si basano su dei termini di servizio standard. E in cui non è difficile la creazione di situazioni comunicative ad-hoc che rispondano alle misure governative. Insomma, uno scenario non facile, [anche perché] l'universo PlayStation è solo uno dei fronti elettronici possibili, i sistemi di gioco *online* sono molti e tutti hanno i loro labirinti. In cui non è difficile nascondersi». TONIUTTI, *Terrorismo, Orlando: "Intercettazioni anche su chat e PlayStation"*, www.repubblica.it, 26 novembre 2015.

[492] 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 software (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. Il programma software per chiamate VoIP più diffuso al mondo è Skype.

dalle distinte caratteristiche del sistema oggetto delle attività di captazione, nonché dal tipo di informazioni che si intendono acquisire.

L'intercettazione del contenuto delle e-mail avviene tecnicamente attraverso la duplicazione dell'account oggetto di monitoraggio: si tratta di una vera e propria clonazione della cassetta di posta elettronica dell'utente con un adeguato sistema di *forwarding* presso la postazione di decodifica[493]. Da un punto di vista squisitamente giuridico, mentre è pacifica la riconducibilità della captazione del flusso comunicativo nell'ambito della disciplina delle intercettazioni telematiche, così come è fuori discussione la possibilità di ricorrere alla disciplina del sequestro in ipotesi di acquisizione del contenuto di email "già lette" dal destinatario, maggiori problemi crea il caso, tutt'altro che infrequente, dell'acquisizione dei messaggi di posta elettronica temporaneamente memorizzati presso l'Internet *service provider* in attesa di essere "lette" dal destinatario[494]. In questo caso, la mail si trova in *stand by,* allocata presso il server del destinatario, ma non ancora concretamente giunta a destinazione. Ebbene, una parte della dottrina appare orientata a ritenere applicabile a tale ipotesi la disciplina del sequestro di cui agli artt. 254 co. 1 c.p.p. e 254-*bis* c.p.p., poiché tali previsioni consentono la possibilità di sequestrare presso i fornitori di servizi telematici o di telecomunicazioni corrispondenza inoltrata per via telematica e che si deve supporre non ancora conosciuta dal destinatario[495], salvo recuperare la disciplina più garantista di cui all'art. 266-*bis* c.p.p. quando, invece, la mail transita dal server del ricevente al contenitore virtuale detto "casella di posta elettronica" dell'utente[496]. In altre parole, il flusso comunicativo dinamico si apprende tramite intercettazione telematica, mentre la corrispondenza elettronica statica (allocata nel server o già arrivata e letta dal destinatario finale) si acquisisce tramite sequestro.

---

[493] L'*email forwarding* è un servizio fornito dal *web provider*: fa sì che quando un utente invia una email ad una casella di posta, il sistema "rigira" la suddetta email ad un altro account appartenente ad un altro utente. Tale metodo è ovviamente indispensabile quando l'indirizzo di posta elettronica è l'unico elemento investigativo su cui si può operare.

[494] Su questo specifico aspetto, cfr. R. ORLANDI, *Questioni attuali in tema di processo ed informatica*, in *Riv. dir. proc.*, 2009, p. 135, nonché L. LUPARIA, *Computer crimes e procedimento penale*, in G. GARUTI (a cura di), *Modelli differenziati di accertamento,* in *Trattato di procedura penale*, diretto da G. SPANGHER, vol. VII, Torino, 2011, p. 387.

[495] R. E. KOSTORIS, *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in AA.VV, *Nuove tendenze di giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, L. RUGGERI - L. PICOTTI (a cura di), Torino, 2011, p.180.

[496] R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, cit., p.134; E. M. MANCUSO, *L'acquisizione di contenuti e-mail,* cit., p.69.

Quanto alle chat ed alle conversazioni vocali tramite tecnologia Voip, le tradizionali intercettazioni "passive" -ossia le intercettazioni del traffico dati su linea (telefonica fissa – adsl – e cellulare – umts – definite genericamente "passive") che si basano sulla cattura del traffico duplicato dal provider di telecomunicazioni (gestore) che assicura un servizio di connettività all'indagato- non sono in grado di fornire informazioni e dati degni di interesse, in quanto la maggior parte del traffico risulta cifrato: in pratica le intercettazioni su linea fissa (ADSL) e mobile (UMTS) permettono solo di accertare che i dispositivi in uso all'indagato sono effettivamente utilizzati, ma non consentono nella stragrande maggioranza dei casi di fornire dati rilevanti[497]. Per tale motivo gli organismi specializzati dei servizi centrali di polizia giudiziaria, con l'ausilio di società di settore, utilizzano tecnologie in grado di intercettare le informazioni nelle fasi in cui sono in chiaro, ossia dopo la decodifica, direttamente all'interno dei dispositivi. Tali tecniche vengono generalmente denominate "intercettazioni attive", in quanto presuppongono non più soltanto un ascolto passivo del segnale, ma anche un'attività di cattura dell'informazione. In sostanza, l'attività di captazione si sposta dalla linea all'interno del dispositivo, trasformandosi da intercettazione del flusso in cattura del dato presente nel dispositivo, attraverso veri e propri captatori informatici[498]. Ovviamente, la copertura normativa dell'intercettazione prevista dagli art. 266 e seguenti del c.p.p. regge a patto che oggetto della captazione sia una comunicazione (intesa in senso lato, se si vuole, ma pur sempre comprendente dati c.d. comunicativi) e non anche dati e informazioni già presenti e memorizzati all'interno dei dispositivi attenzionati (c.d. dati non comunicativi).

2. Virus informatico, intercettazioni ambientali e videoriprese

Quanto detto aiuta a comprendere meglio la realtà che stiamo vivendo: il captatore informatico, inteso come strumento software in grado di "perquisire" ed acquisire a distanza il contenuto informativo di qualsiasi dispositivo di memorizzazione digitale connesso alla rete

[497] Se non i c.d. "dati esterni", una sorta di tabulato di traffico, molto parziale (traffico verso un determinato sito, senza informazioni di dettaglio sui contenuti dell'esplorazione).
[498] Cfr. P. ANGELOSANTO, *Le intercettazioni telematiche e le criticità del data retention nel contrasto alla criminalità organizzata, Atti del convegno "Intercettazioni, tra esigenze investigative e diritto alla privacy"* – Palermo, 17-18 gennaio 2014, su www.sicurezzaegiustizia.com.

Internet, rappresenta solo una *species* dei possibili utilizzi per fini investigativi dei c.d. *trojan* di Stato. All'interno della generale categoria dei *remote control systems,* esistono programmi in grado di acquisire furtivamente la totalità delle funzioni esplicabili attraverso un dispositivo digitale. In particolare, è divenuto sempre più frequente il ricorso ai *trojan horse* per la realizzazione di vere e proprie intercettazioni ambientali e di videoriprese investigative.

Queste "microspie telematiche" rappresentano l'evoluzione tecnologica delle "vecchie" microspie per intercettazioni ambientali che venivano fisicamente piazzate nei luoghi di pertinenza dell'indagato, con il vantaggio, non secondario per chi materialmente deve procedere all'installazione, di evitare qualsiasi contatto fisico con la persona sottoposta alle indagini: le nuove microspie viaggiano sul web e si auto-installano furtivamente sullo *smartphone* dell'indagato, prendendo il controllo del microfono e della microcamera del dispositivo.

Dal punto di vista investigativo, i vantaggi di questo nuovo strumento sono evidenti: non solo si azzera il rischio, sempre presente, di essere scoperti, vanificando irrimediabilmente le indagini in corso, ma si ottiene anche un risultato estremamente più efficace: la "cimice", infatti, non è più fissa in un luogo, ma segue l'indagato in ogni suo spostamento, consentendone un monitoraggio audio-video in ogni dove.

Dal punto vista giuridico, tuttavia, è necessario interrogarsi sulla legittimità di tale opzione investigativa, alla luce, questa volta, delle norme in vigore, sia di rango ordinario[499] che costituzionale[500]. Un interessante stimolo in questo senso proviene da un recente *decisum* della giurisprudenza di legittimità che tenta di fare il punto della situazione, sia con riferimento al tema delle intercettazioni ambientali, sia relativamente a quello delle videoriprese, entrambi realizzabili mediante l'attivazione da remoto del microfono e della telecamera di uno *smarthpone*[501].

[499] Il riferimento, qui, quantomeno con riferimento all'intercettazione audio, è all'art. 266, co. 2, c.p.p.
[500] Cfr. art. 15 Cost.
[501] Cfr. Cass., sez. VI, 26 maggio 2015, n. 27100, in *Mass. red.*, 2015.

2.1 Sulle intercettazioni ambientali tramite virus informatico

Nel caso deciso dalla Suprema Corte, uno degli imputati[502] ricorre per cassazione avverso l'ordinanza del Tribunale del riesame confermativa dell'ordinanza applicativa della misura intramurale, deducendo violazione di legge e vizio di motivazione «in quanto il pubblico ministero, in relazione alle utenze telefoniche in uso ai coimputati […] ha disposto sia l'intercettazione d'urgenza telematica, tramite agente intrusore (virus informatico), di tutto il traffico dati, in relazione agli apparecchi utilizzati dai predetti, sia di tutte le conversazioni tra presenti, mediante l'attivazione, attraverso il predetto virus, del microfono e della videocamera dei relativi Smartphone»[503]. Ciò, secondo il ricorrente, «al di là di una invasiva e illegittima apprensione dei contenuti della memoria dei predetti apparecchi cellulari […], operazione esulante dalla normativa prevista in tema di intercettazioni», ha comportato una intercettazione *sui generis,* in contrasto con quanto previsto dalle norme del codice di rito e, di conseguenza, foriera di risultati inutilizzabili: «utilizzando il sistema del virus informatico sul telefono cellulare, le intercettazioni effettuate non sono soggette ad alcuna restrizione nè temporale nè spaziale. Il telefono cellulare è divenuto ormai oggetto che accompagna ogni nostro movimento ed è in grado, se utilizzato con finalità captatorie, di sottoporre l'individuo ad un indiscriminato controllo, non solo di tutta la sua vita privata ma anche dei soggetti che gli stanno vicino. L'intercettazione potrà dunque divenire ambientale e anche effettuarsi all'interno di un domicilio, poiché il telefono cellulare diviene un microfono e la sua telecamera una spia video. D'altronde, nel decreto del Gip non si fa riferimento alla possibilità che il detto strumento venga utilizzato anche all'interno delle private dimore dei soggetti intercettati e, comunque, non vi è alcuna indicazione dei luoghi e dei tempi della predetta captazione»[504].

Ebbene, la Corte di cassazione, investita della questione nel procedimento incidentale *de libertate*, afferma in maniera perentoria che «non sembra potersi dubitare che l'art. 266 c.p.p., comma 2, nel contemplare l'intercettazione di comunicazioni tra presenti, si riferisca alla captazione di conversazioni che avvengano in un determinato luogo e non ovunque». Avallando la tesi difensiva, la Corte continua osservando come «una corretta ermeneutica

---

[502] L'ipotesi di reato contestata è l'art. 416-*bis* c.p., per avere partecipato all'associazione di tipo mafioso, armata, operante in Biancavilla e denominata "clan Mazzaglia- Toscano-Tomasello", affiliata alla famiglia catanese di Cosa Nostra Santapaola- Ercolano.
[503] Cfr. Cass, sez. VI, 26 maggio 2015, n. 27100, cit.
[504] *Ibidem*.

della norma di cui all'art. 15 Cost. osta infatti all'attribuzione al disposto dell'art. 266 c.p.p., comma 2 di una latitudine operativa così ampia da ricomprendere intercettazioni ambientali effettuate in qualunque luogo. La norma costituzionale pone infatti il fondamentale principio secondo il quale la libertà e la segretezza delle comunicazioni sono inviolabili, ammettendo una limitazione soltanto per atto motivato dell'autorità giudiziaria e con le garanzie stabilite dalla legge. Ne deriva che le norme che prevedono la possibilità di intercettare comunicazioni tra presenti sono di stretta interpretazione, ragion per cui non può considerarsi giuridicamente corretto attribuire alla norma codicistica una portata applicativa così ampia da includere la possibilità di una captazione esperibile ovunque il soggetto si sposti. Viceversa, l'unica opzione interpretativa compatibile con il dettato costituzionale è quella secondo la quale l'intercettazione ambientale deve avvenire in luoghi ben circoscritti e individuati *ab origine* e non in qualunque luogo si trovi il soggetto»[505].

La conseguenza è ovvia: poiché «nel caso di specie, la tecnica utilizzata consente, attraverso l'attivazione del microfono del telefono cellulare, la captazione di comunicazioni in qualsiasi luogo si rechi il soggetto, portando con sè l'apparecchio», essa «non è giuridicamente ammissibile». Ciò in quanto, non siamo di fronte ad una «semplice modalità attuativa del mezzo di ricerca della prova, costituito dalle intercettazioni», quanto, piuttosto, ad «una tecnica di captazione che presenta delle specifiche peculiarità e che aggiunge un *quid pluris*, rispetto alle ordinarie potenzialità dell'intercettazione, costituito, per l'appunto, dalla possibilità di captare conversazioni tra presenti non solo in una pluralità di luoghi, a seconda degli spostamenti del soggetto, ma -ciò che costituisce il fulcro problematico della questione- senza limitazione di luogo. Ciò è inibito, prima ancora che dalla normativa codicistica, dal precetto costituzionale di cui all'art. 15 Cost.[506]».

A fronte di questo arresto giurisprudenziale, in dottrina i pareri sono discordi. In base ad un primo convincimento[507], la decisione della Suprema Corte non convince né dal punto vista tecnico, né sotto il profilo giuridico. Quanto al primo aspetto, si sostiene, i giudici di legittimità non riescono a cogliere la specificità tecnica delle intercettazioni ambientali rispetto alle intercettazioni telefoniche: mentre queste ultime presuppongono l'esistenza di una specifica apparecchiatura o di un particolare sistema da sottoporre a controllo, le seconde,

---

[505] *Ibidem*.
[506] *Ibidem*.
[507] G. AMATO, *L'intercettazione ambientale non può avvenire in qualunque luogo si trovi il soggetto*, in *Il Sole 24 Ore*, 5 ottobre 2015.

disciplinate dal comma 2 dell'articolo 266 c.p.p., «per la loro intrinseca natura non necessitano della individuazione degli apparecchi, ma si riferiscono ad ambienti in cui deve intervenire la captazione, con la conseguenza che devono considerarsi legittime, con possibilità di piena utilizzazione dei risultati, anche quando in corso di esecuzione intervenga una variazione dei luoghi in cui deve svolgersi la captazione»[508]. Dal punto di vista giuridico, tale differenza si riflette in punto di adeguata motivazione del decreto autorizzativo dello svolgimento delle operazioni di intercettazione: nel caso di intercettazioni telefoniche, il provvedimento dovrà contenere indefettibilmente le specifiche degli apparati oggetto di controllo; in ipotesi di intercettazioni ambientali, invece, il decreto deve specificamente indicare le situazioni ambientali oggetto di monitoraggio. Ma, ed è questo il punto di maggiore interesse, secondo l'opinione in commento «la motivazione deve considerarsi adeguata anche in presenza del semplice riferimento ai luoghi (comunque) frequentati dal possessore dell'apparecchio su cui è stato installato l'agente intrusore»[509]. Coerentemente con tale ragionamento, la possibilità di ricorrere ad un decreto autorizzativo che tenga conto della dinamicità del controllo con l'interessamento di ambienti diversi, ma comunque frequentati dal soggetto sottoposto a controllo, fa perdere di vista la differenza tra intercettazioni ambientali tradizionali e intercettazioni audio svolte tramite *virus* informatico: «il richiamo operato dalla Corte ai principi costituzionali appare generico e aspecifico, non riuscendosi a cogliere quel plus di intrusione, rispetto a una intercettazione ambientale classica (ergo, disposta in un ambiente ben determinato e immutabile) [di una intercettazione tramite captatore informatico…]. Ciò che rileva [...è...] l'adeguatezza della motivazione del provvedimento autorizzativo, che spieghi cioè la metodica tecnica utilizzata e quindi giustifichi la mobilità/dinamicità delle operazioni captative[510]».

Di diverso avviso, altra dottrina[511] saluta con favore il *decisum* in commento. Pur riconoscendo che l'autorizzazione del Giudice per le indagini preliminari a disporre le intercettazioni ambientali *de quibus* «si pone in perfetta sintonia con i principi cardine del nostro sistema e, quindi, con quell'affievolimento del fondamentale diritto alla riservatezza e della inviolabilità del domicilio realizzabile attraverso un provvedimento motivato dell'Autorità giurisdizionale», tale opinione ritiene permangano dei dubbi relativamente alle

---

[508] *Ibidem*.
[509] *Ibidem*.
[510] *Ibidem*.
[511] Cfr. A. TESTAGUZZA, *I sistemi di controllo remoto: fra normativa e prassi*, cit., p. 759.

modalità di svolgimento delle operazioni in esame. Ed infatti, «se è vero […] che deve ritenersi esclusa una predeterminazione a priori dei luoghi ove realizzare l'intercettazione[512] […] è anche vero, di converso, che l'impossibilità di determinarli con esattezza non esclude il rischio di aggiramento degli stessi limiti imposti dalla pronuncia in esame. […] L'impossibilità di stabilire con esattezza gli spostamenti dello strumento elettronico e la garanzia offerta agli inquirenti di poter comunque svolgere un'attività di intercettazione ambientale, debitamente autorizzata, non può che stridere con le prerogative di riservatezza sancite a livello costituzionale. […] Consentire, dunque, all'interno di un decreto di autorizzazione alle intercettazioni la possibilità di svolgerle in ogni luogo (ad eccezione di quelli di privata dimora) pur nella consapevolezza della potenziale mobilità dello strumento utilizzato per la captazione, renderebbe del tutto vano lo sforzo, promosso in sede costituente, di disciplinare un'autorizzazione preventiva da parte dell'Autorità giurisdizionale per la limitazione del diritto inviolabile di libertà e segretezza della comunicazione. In caso contrario (si giustifichi la provocazione) basterebbe autorizzare sempre e comunque tali attività, contando sulla sola esistenza dei gravi indizi di reato e dell'indispensabilità del mezzo ai fini della prosecuzione delle indagini, riservando la verifica dei presupposti previsti dal comma 2 dell'art. 266 c.p.p. in un momento successivo. Ma non sembra questa una lettura conforme al dettato costituzionale»[513].

2.2 Sulle videoriprese

La seconda problematica concerne l'attivazione, da remoto, della telecamera del telefono cellulare al fine di monitorare a livello visivo il comportamento e l'atteggiarsi del soggetto indagato. Come noto, il tema dell'utilizzo di videoriprese occulte per fini investigativi[514], lungi dall'essere stato disciplinato positivamente, è ancor oggi regolamentato dal diritto vivente. In estrema sintesi, in base a quanto chiarito dalla Corte costituzionale[515] e dalle

[512] Anche e soprattutto sulla base di precedenti orientamenti giurisprudenziali secondo i quali «l'intercettazione di comunicazioni tra presenti richiede l'indicazione dell'ambiente nel quale l'operazione deve avvenire solo quando si tratti di abitazioni o luoghi privati, secondo l'indicazione di cui all'art. 614 c.p.». Così, Cass., Sez. VI, 2 dicembre 1999, Bembi ed altro, n. 3541, in *CED Cass.*, rv. 214972.
[513] Cfr. A. TESTAGUZZA, *I sistemi di controllo remoto*, cit., p. 759.
[514] Per un approfondimento, cfr. C. MARINELLI, *Intercettazioni processuali e nuovo mezzi di ricerca della prova*, cit., pp. 159 e ss.
[515] Corte costituzionale, sent. n. 135/2002 e n. 149/2008, in www.giurcost.org.

Sezioni Unite della Corte di cassazione[516], le videoregistrazioni in luoghi pubblici o aperti o esposti al pubblico, non effettuate nell'ambito del procedimento penale, vanno incluse nella categoria dei documenti, *ex* art. 234 cod. proc. pen. Le predette registrazioni, se vengono invece effettuate dalla p.g., anche d'iniziativa, vanno incluse nella categoria delle prove atipiche e sono pertanto soggette alla disciplina dettata dall'art. 189 c.p.p. Con la seguente precisazione: esse non possono essere espletate ovunque; le videoregistrazioni effettuate in ambito domiciliare, ai fini del procedimento penale, sono acquisite illecitamente e sono perciò inutilizzabili, anche se la tutela costituzionale del domicilio va limitata ai luoghi con i quali la persona abbia un rapporto stabile; sicché, quando si tratta di tutelare la sola riservatezza, la prova atipica può essere ammessa con provvedimento motivato dell'autorità giudiziaria. Devono dunque essere oggetto di tutela da parte dell'autorità giudiziaria (pubblico ministero o giudice) le riprese visive che, pur non comportando intrusione domiciliare, violino la riservatezza personale (come, ad esempio, le riprese effettuate dalla polizia giudiziaria in un bagno pubblico).

Relativamente al caso di specie, ne deriva «che occorre verificare che, mediante l'attivazione da remoto della telecamera inerente al telefono cellulare, non siano state effettuate videoregistrazioni all'interno di luoghi di privata dimora o, comunque, tali da imporre la necessità di tutelare la riservatezza personale […]. Nell'affermativa, anche queste risultanze dovranno essere espunte dal compendio indiziario. Si tratta infatti di una questione non di legittimità della tecnica di acquisizione probatoria, in sè considerata, ma di utilizzabilità delle relative risultanze»[517].

[516] Sul tema delle videoriprese, cfr. Cass., sez. un., 28 marzo 2006, Prisco, in *CED Cass.*, n. 234267.
[517] Cfr. Cass., sez. VI, 26 giugno 2015, n. 27100, cit.

CAPITOLO 5
Il PEDINAMENTO ELETTRONICO

Sommario: 1. Premessa - 2. La natura giuridica dell'attività di geolocalizzazione - 3. La disciplina applicabile - 4. Profili critici

1. Premessa

Il c.d. "pedinamento" rappresenta il più tradizionale, e tuttavia sempre attuale, strumento di indagine di cui fa uso la polizia giudiziaria nel corso delle indagini preliminari. Tecnicamente, esso consiste nel «seguire una persona con circospezione allo scopo di spiarne le mosse»[518]. La persona oggetto di pedinamento può essere sia l'indagato, sia altri soggetti i cui movimenti siano ritenuti utili ai fini delle indagini[519]. Giuridicamente, il pedinamento è ascrivibile tra gli atti investigativi atipici: esso può essere svolto a piedi[520] o tramite mezzi di locomozione, ciò che conta è che sia fatto con "circospezione", ossia in modo occulto, atteso che dal punto di vista investigativo la sua utilità dipende esclusivamente dal fatto che la persona seguita non si accorga di esserlo[521]. Distinta dal pedinamento è l'attività c.d. di "appostamento", che si caratterizza per il carattere fisso della postazione di controllo[522].

Ebbene, l'evoluzione tecnologica ha interessato da vicino anche l'attività di indagine atipica di pedinamento. In particolare, è sempre più diffuso nella prassi investigativa l'utilizzo di sistemi tecnologici di localizzazione a distanza di una persona o di una cosa: pur rimanendo costante la funzione tradizionale (il fatto di seguire qualcuno), il pedinamento diventa "elettronico"[523], nel senso che gli spostamenti della persona da monitorare vengono seguiti da

---

[518] N. ZINGARELLI, *sub pedinare*, in M. CANNELLA – B. LAZZARINI (a cura di), *Lo Zingarelli 2015. Vocabolario della lingua italiana*, 2015, p. 1357.

[519] Ad esempio, in un procedimento per sequestro di persona a scopo di estorsione, può essere utile, al fine di individuare gli autori del reato, monitorare gli spostamenti dei familiari della vittima.

[520] Etimologicamente, la parola deriva dal verbo "pedinare", perché inizialmente il soggetto attenzionato veniva seguito esclusivamente a piedi.

[521] Gli accorgimenti per evitare di essere "scoperti" sono diversi e mutano in ragione del tipo di pedinamento: a piedi, ad esempio, è utile seguire a distanza la persona senza mai fissarla negli occhi, evitando di attirare l'attenzione (magari con vestiti troppo appariscenti); in auto, il pedinamento richiede la partecipazione di almeno due autovetture che si alternino nel monitoraggio; ecc.

[522] Cfr. A. MORGIGNI, *L'attività di polizia giudiziaria*, Milano, 2002, pp. 527 e ss.

[523] Cfr, fra i tanti contributi, C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., pp. 227 e ss.

remoto attraverso strumenti elettronici, senza la necessaria presenza fisica degli operatori sul posto.

Dal punto di vista tecnico, il monitoraggio a distanza può avvenire tramite sistemi di tipo satellitare o sfruttando la localizzazione cellulare. Con riferimento ai primi, merita di essere segnalato il c.d. *g.p.s.*, acronimo di *global positioning system*, in grado di determinare con estrema precisione la posizione –espressa in coordinate di latitudine, longitudine e altezza- di un oggetto sulla superficie terrestre, nonché di seguirne il movimento e calcolarne la velocità, sfruttando una rete di 24 satelliti collocati a circa 20.000 km di altezza e suddivisi in 6 rotte orbitali. La localizzazione avviene tramite la trasmissione di un segnale radio da parte di ciascun satellite e l'elaborazione dei segnali ricevuti da parte del ricevitore sulla Terra[524]. L'impiego di tale strumento per finalità investigative è reso possibile, di norma, grazie all'installazione "furtiva" della stazione ricevente il segnale satellitare sull'autovettura del soggetto da monitorare.

La localizzazione tramite cellulare, invece, sfrutta il sistema di "celle" in cui risulta ripartito il territorio terrestre coperto dalla telefonia mobile: si analizza la potenza del segnale radio di ogni cella telefonica in relazione alla rispettiva stazione radio base (che ha coordinate geografiche note) collegata con il dispositivo mobile o terminale e ne viene determinata la distanza da questa in base alla conoscenza dell'attenuazione dell'ambiente di radiopropagazione[525]. L'utilizzo investigativo di questo tipo di monitoraggio non necessita di supporti: è sufficiente che la persona da monitorare porti con sé, nei suoi spostamenti, lo *smarthphone* o il *tablet* dotato di connessione mobile.

Ebbene, è fuori discussione che dal punto di vista tecnico-operativo gli strumenti di monitoraggio ad alto contenuto tecnologico abbiano trasformato la tradizionale fisionomia dell'attività di pedinamento, facilitando senz'altro il lavoro degli investigatori. Tuttavia, questi mezzi di indagine pongono nuovi problemi interpretativi dal punto di vista giuridico-processuale. In particolare, dottrina e giurisprudenza si interrogano da tempo, senza giungere

---

[524] Il sistema GPS è gestito dal governo degli Stati Uniti d'America ed è liberamente accessibile da chiunque sia dotato di un ricevitore GPS. Il suo grado attuale di accuratezza è dell'ordine dei metri, in dipendenza dalle condizioni meteorologiche, dalla disponibilità e dalla posizione dei satelliti rispetto al ricevitore, dalla qualità e dal tipo di ricevitore, dagli effetti di radiopropagazione del segnale radio in ionosfera e troposfera (es. riflessione) e dagli effetti della relatività. Per un maggiore approfondimento, che non è il caso di proseguire in questa sede, si rinvia al seguente url: www.gps.gov.

[525] Cfr. voce *Geolocalizzazione*, in *www.vikipedia.org*. Per un approfondimento di natura tecnica, cfr. R. OLIVIERI, *I sistemi di geolocalizzazione e l'analisi forense degli smartphone*, in G. COSTABILE – A. ATTANASIO – M. IANULARDO (a cura di), *IISFA Memberbook 2014. Digital forensics. Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER*, Forlì, 2015, pp. 141 e ss.

peraltro a soluzioni condivise, sui temi della natura giuridica e, conseguentemente, della disciplina applicabile al sistema di geolocalizzazione[526], chiedendosi se si tratti di attività atipica riconducibile, al pari del pedinamento tradizionale, agli articoli 55, 347 e 370 c.p.p., o se, piuttosto, il mezzo elettronico conferisca all'atto del pedinare un *quid pluris* potenzialmente in grado di stravolgerne la tradizionale natura. Ammesso poi che si tratti di prova atipica, occorre capire se è davvero sufficiente l'iniziativa della polizia giudiziaria o se piuttosto sia necessario (e sufficiente) ricorrere al meccanismo dell'art. 189 c.p.p. e al provvedimento motivato dell'autorità giudiziaria[527]. Se, viceversa, di tratta di prova tipica, ci si chiede quale sia la sua corretta collocazione nell'ambito dei tradizionali e tipici mezzi di ricerca della prova.

2. La natura giuridica dell'attività di geolocalizzazione

Il primo quesito da risolvere attiene alla riconducibilità, o meno, del pedinamento elettronico ad uno dei mezzi di ricerca della prova previsti espressamente nel codice di rito. Le potenziali categorie di appartenenza che hanno attratto l'attenzione degli interpreti sono tre: le ispezioni personali di cui all'art. 244, co. 1, c.p.p., gli accertamenti di polizia giudiziaria *ex* art. 354 c.p.p. e le intercettazioni previste dagli artt. 266 e ss. c.p.p.

Una voce, peraltro rimasta isolata, della dottrina ha ritenuto assimilabile il pedinamento tramite *g.p.s.* ad un'ispezione personale in ragione della sua idoneità a consentire di «osservare elettronicamente» gli spostamenti di una persona, a discapito dell'art. 13 Cost.[528]. Senonché, il dato testuale è in grado da solo di confutare tale opinione: l'operazione ispettiva è finalizzata ad accertare le «tracce e gli altri effetti materiali del reato» o, al più, a descrivere lo stato attuale o preesistente dei luoghi, di tal ché è da escludere che il pedinamento satellitare possa essere inquadrato nell'art. 244, co. 1, c.p.p.[529]

Anche la comparazione con gli accertamenti ed i rilievi che la polizia giudiziaria è legittimata a svolgere a norma dell'art. 354 c.p.p. ha dato un prevedibile esito negativo. Oltre

---

[526] La geolocalizzazione, in generale, è l'identificazione della posizione geografica nel mondo reale di un dato oggetto.
[527] Cfr., Corte costituzionale, sentenze n. 81 del 1993, n. 366 del 1991 e n. 281 del 1998, in www.giurcost.org.
[528] Così, L. CARLI, *Le indagini preliminari nel sistema processuale penale*, cit., p. 333.
[529] Peraltro, la fisiologica natura occulta del pedinamento sarebbe incompatibile con il previo avviso di cui all'art. 245, co. 1, c.p.p. Cfr., S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.*, 2012, p. 586.

alle differenze strutturali e funzionali, ha giocato un ruolo determinante in questo senso il carattere palese e garantito di tali attività di indagine[530]: «l'obbligo del previo avviso all'interessato della facoltà di farsi assistere dal difensore eliminerebbe alla radice -per intuibili ragioni- la possibilità di compiere l'accertamento stesso»[531]. Nemmeno la soluzione di limitare l'obbligo di avviso esclusivamente alle fattispecie in cui l'atto da compiere coinvolga "fisicamente" l'indagato[532] appare convincente, poiché la forzatura del dato normativo rimarrebbe comunque evidente. A ciò si aggiunga la considerazione per cui le operazioni tecniche di doverosa iniziativa della polizia giudiziaria *ex* art. 354 c.p.p. non risentono (com'è ovvio) «di alcuna limitazione in ordine alla tipologia della fattispecie di reato ipotizzata dall'accusa ed alla valutazione dell'indispensabilità o meno dell'atto da compiere»; tali caratteristiche, fisiologiche nel caso di accertamenti urgenti, «mal si conciliano con la natura di accertamento particolarmente intrusivo ed occulto del sistema di osservazione e controllo g.p.s., la cui utilizzazione, pertanto, deve essere più rigorosamente circoscritta»[533].

Quanto alla possibile riconducibilità del pedinamento elettronico alle intercettazioni, la risposta negativa a tale interrogativo non è apparsa di così immediata percezione. I motivi che ne spiegano la "vicinanza" sono presto detti: la "affinità" degli strumenti tecnici di captazione[534]; l'avvertita esigenza di assicurare, in caso di monitoraggio elettronico così come in ipotesi di intercettazione, il rispetto della riserva di legge e della riserva di giurisdizione[535]; la non sempre chiara delimitazione del concetto stesso di intercettazione di comunicazioni, spesso dilatato al punto da ricomprendere al suo interno oggetti eterogenei[536]. Nonostante tali indiscutibili punti di contatto, esistono obiezioni insuperabili che spingono a favore della impossibilità di ricondurre normativamente il pedinamento elettronico alle intercettazioni.

---

[530] In dottrina, cfr. C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p. 234.
[531] L.G. VELANI, *Nuove tecnologie e prova penale: il sistema di individuazione satellitare g.p.s.*, in *Giur. it.*, 2003, p. 2372.
[532] CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, cit., p. 1196.
[533] Così, L.G. VELANI, *Nuove tecnologie e prova penale: il sistema di individuazione satellitare g.p.s*, cit., p. 2372.
[534] Cfr. C. MARINELLI, *Intercettazioni processuali*, cit., p. 234.
[535] Secondo una parte della dottrina, la localizzazione satellitare andrebbe concepita come una particolare tipologia di intercettazione sul presupposto che il suo impiego determina una lesione della privacy del soggetto monitorato. Cfr., VELANI, *Nuove tecnologie e prova penale: il sistema di individuazione satellitare g.p.s.*, cit., p. 2375; IACOBACCI, *Sulla necessità di riformare la disciplina delle intercettazioni prendendo le mosse dalle esitazioni applicative già note*, in *Giust. pen.*, 2011, III, p. 365.
[536] Cfr. P. PERETOLI, *Controllo satellitare con G.P.S.: pedinamento o intercettazione?*, in *Dir. pen. proc.*, 2003, I, p. 96.

Innanzitutto, è diverso l'oggetto della captazione: il contenuto di una comunicazione tra due o più persone, in caso di intercettazione[537]; la posizione e gli spostamenti di una persona o di una cosa, in ipotesi di geolocalizzazione[538]; e il discorso non cambia nemmeno in ipotesi di comunicazioni informatiche o telematiche contemplate dall'art. 266-*bis* c.p.p.[539]. Inoltre, dal punto di vista soggettivo, una cosa è la occulta presa di conoscenza, da parte di un terzo, del contenuto di una comunicazione riservata, intercorrente tra due o più soggetti; ben altra cosa è la mera ricezione di un segnale automatico alla cui produzione il localizzando non contribuisce minimamente; in quest'ultimo caso, infatti, non solo l'interessato «non comunica intenzionalmente con alcuno»[540], ma neppure può essere ritenuto l'autore della trasmissione captata e rilevatrice delle informazioni riguardanti la sua posizione e i suoi spostamenti[541].

Sulla natura giuridica, dunque, è meritevole di accoglimento quell'orientamento della giurisprudenza di legittimità che, sin dal 2002, qualifica in termini di atipicità il pedinamento elettronico: «la localizzazione di una persona (o di un oggetto) in movimento mai può essere considerata una attività di intercettazione, anche se realizzata con modalità e tecnologie similari a quelle con le quali vengono portate ad esecuzione, appunto, le intercettazioni previste dal codice di rito»[542]. Tale conclusione, secondo la Suprema corte, deriva proprio dall'eterogeneità dell'oggetto di apprensione. Di conseguenza, la Corte ha definito la geolocalizzazione «una modalità, tecnologicamente caratterizzata, di pedinamento», ascrivendola al *genus* dei mezzi di ricerca della prova atipici o innominati, di competenza

---

[537] Sulla definizione di intercettazione, cfr. Cass., sez. un., 24 settembre 2003, Torcasio, cit., p. 2094, con nota di L. FILIPPI, *Le sezioni unite decretano la morte dell'agente segreto attrezzato per il suono*.

[538] Cfr. P. TONINI, *Manuale di procedura penale*, cit., p. 391, il quale sottolinea come sia estraneo all'intercettazione, perché non ha per oggetto una comunicazione, il pedinamento mediante apparecchiatura satellitare G.P.S. In dottrina, cfr. anche C. BOTTI, *Ma il sensore posto nell'autoveicolo potrebbe violare il domicilio?*, in *Dir. & giust.*, 2002, 22, p. 17; E. APRILE – F. SPIEZIA, *Le intercettazioni telefoniche e ambientali*, cit., p. 154; C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, cit., p. 239; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova nell'attività di polizia giudiziaria: videosorveglianza, pedinamento e localizzazione satellitare*, in *Riv. polizia*, 2007, p. 672; G. DI PAOLO, *"Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, cit., p. 252. M. STRAMAGLIA, *Il pedinamento satellitare: ricerca ed uso di una prova "atipica"*, in *Dir. pen. proc.*, 2011, p. 214; S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, cit., p. 584.

[539] «Se infatti appare intuitiva l'impossibilità di ricondurlo [il flusso di dati ottenuto attraverso il sistema di geolocalizzazione] all'oggetto delle captazioni di cui all'art. 266 c.p.p., non venendo in rilievo conversazioni o comunicazioni telefoniche, né altre forme di telecomunicazione a queste assimilabili per il mancato coinvolgimento di due o più persone, parimenti arbitrario sarebbe l'inquadramento nel novero delle comunicazioni telematiche o informatiche contemplate dall'art. 266-*bis* c.p.p.. Non si è in presenza infatti di una trasmissione di dati tra elaboratori elettronici, né eseguita tramite linee telefoniche». Così, C. MARINELLI, *Intercettazioni processuali*, cit., p. 235.

[540] P. PERETOLI, *Controllo satellitare*, cit., p. 101.

[541] C. MARINELLI, *Intercettazioni processuali*, cit., p. 236.

[542] Cfr. Cass., sez. V, 27 febbraio 2002, Bresciani e altri, in *Dir. pen. proc.*, 2003, I, p. 93.

della polizia giudiziaria ai sensi degli artt. 55, 347 e 370 c.p.p. Infatti, non venendo in rilievo una potenziale lesione del bene giuridico della libertà e della segretezza delle comunicazioni (art. 15 Cost.), non è necessario alcun controllo dell'autorità giudiziaria[543].

3. La disciplina applicabile

Il richiamo fatto dalla Corte di cassazione agli articoli 55, 347 e 370 c.p.p. non esaurisce il tema della disciplina giuridica applicabile al mezzo di ricerca della prova atipico in argomento. Infatti, tali disposizioni «attengono alle attribuzioni degli organi inquirenti […], ma non regolano direttamente il loro concreto esercizio»[544]. Come qualsiasi altro mezzo atipico di ricerca della prova, anche il pedinamento elettronico deve passare attraverso le maglie dell'art. 189 c.p.p., dedicato alle prove non disciplinate dalle legge. Fuori discussione sembra l'idoneità ad assicurare l'accertamento dei fatti: la geolocalizzazione unisce alla valenza del pedinamento tradizionale la maggiore e più efficace attendibilità fornita dalle nuove tecnologie, consentendo un monitoraggio più sicuro[545] e soggetto a minori vincoli spaziali e temporali[546]. Quanto alla tutela della libertà morale della persona, posto che si tratta di uno strumento investigativo occulto e che la sua operatività prescinde da qualsiasi tipo di coercizione e intromissione nella sfera psichica di chi è sottoposto a monitoraggio, sembra impensabile immaginare un nocumento, anche solo potenziale, alla libertà di autodeterminazione o una limitazione delle capacità mnemonico-valutative del soggetto controllato[547]. Infine, il contraddittorio sulle modalità di assunzione deve ritenersi posticipato, in base ad una interpretazione adeguatrice dell'art. 189 c.p.p. che ne consenta l'utilizzo anche con riferimento ai mezzi atipici di ricerca della prova[548].

---

[543] Cfr. Cass., sez. V, 7 maggio 2004, Massa, in *Cass. pen.*, 2005, p. 3016.
[544] C. MARINELLI, *Intercettazioni processuali*, cit., p. 238.
[545] Ed infatti, "l'occhio elettronico" favorisce una maggiore occultabilità delle operazioni rispetto a quelle realizzate alla vecchia maniera, riducendo il rischio di essere scoperti.
[546] L' "occhio elettronico" segue gli spostamenti anche nei luoghi di privata dimora, laddove il pedinamento tradizionale ha un raggio d'azione perlopiù circoscritto ai luoghi pubblici ovvero aperti o esposti al pubblico. Cfr. A. MORGIGNI, *L'attività di polizia giudiziaria*, cit., p. 528.
[547] Cfr. A. LARONGA, *Il pedinamento satellitare: un atto atipico lesivo di diritti inviolabili?*, in *Quest. giust.*, V, 2002, p. 1155.
[548] Cfr. Cass., sez. un., 28 marzo 2006, Prisco, cit., p. 1347.

4. Profili critici

Così come per il captatore informatico[549], anche per il pedinamento elettronico il superamento dell' "esame" dell'art. 189 c.p.p. non mette la parola fine alla questione relativa alla legittimità e, quindi, alla conseguente utilizzabilità dei dati e delle informazioni con esso ottenibili dagli investigatori. Anche in questo caso, vi è l'esigenza di verificare la eventuale esistenza di limiti dovuti alla necessità di tutelare valori costituzionali in conflitto con l'esigenza di accertamento dei reati che giustifica l'utilizzo del sistema di localizzazione in argomento. Infatti, la «disciplina costituzionale assume un triplice rilievo, fungendo nel contempo da limite ermeneutico, da parametro di legittimità e, sia pure in modo più controverso, da fonte di *exclusionary rules*»[550].

In questo caso, l'analisi della eventuale compressione di diritti fondamentali a causa del pedinamento elettronico necessita di una premessa di natura tecnica, che chiarisca la fondamentale differenza tra rilevamento satellitare vero e proprio ed attività propedeutica di tipo preparatorio: il rilevamento consiste nel monitoraggio in tempo reale del segnale satellitare contenente le informazioni relative alla posizione ed allo spostamento del soggetto; l'attività propedeutica si sostanzia nella materiale intrusione all'interno del mezzo da controllare al fine di installare la stazione ricevente il segnale.

Il rilevamento satellitare *tout court* non sembra porre particolari problemi: come già detto, è da escludere, *ratione obiecti,* l'incidenza dell'art. 15 Cost. a causa della inidoneità del mezzo *de quo* ad interferire con la libertà e la segretezza delle comunicazioni[551]; parimenti, sembra fuorviante immaginare una lesione della libertà fisica e psichica del soggetto monitorato, assolutamente ignaro del controllo subito; quanto all'inviolabilità del domicilio, appare arbitraria l'equiparazione della mera localizzazione a condotte analoghe a quelle contemplate dall'art. 614 c.p.[552]. Rimane da indagare la compatibilità dello strumento investigativo rispetto al diritto alla riservatezza, recepito a livello costituzionale dall'art. 2 Cost. Su quest'ultimo aspetto, le idee sono contrastanti: secondo una prima opinione, il diritto alla privacy, estendendosi ad aspetti della vita privata quali «i luoghi frequentati o la circolazione dei singoli sul territorio», non potrebbe ritenersi sufficientemente tutelato in un

---

[549] Cfr., *infra*, in questo capitolo, sez. I, par. 2.3.
[550] Così, C. MARINELLI, *Intercettazioni processuali*, cit., p. 245.
[551] Cass., sez. V, 10 marzo 2010, Z.B., in *Dir. pen. proc.*, 2010, p. 1464; Cass., sez. I, 9 marzo 2010, Congia, in *Mass. Uff.*, n. 246774; Cass., sez. VI, 11 aprile 2008, Sitzia, in *Mass. Uff.*, n. 239638.
[552] C. MARINELLI, *Intercettazioni processuali*, cit., p. 262.

sistema che ammetta una localizzazione satellitare senza limiti[553]; inoltre, «sul piano dei diritti fondamentali […] non può negarsi che l'impiego del sistema di localizzazione g.p.s. abbia realizzato, ad ogni modo, un'interferenza nel diritto alla vita privata tutelato dall'art. 8 C.E.D.U»[554]; secondo un altro orientamento, invece, la genericità dell'art. 2 Cost. comporta il necessario ricorso ad altre disposizioni costituzionali al fine di individuare la esatta area di copertura del diritto alla riservatezza: «occorre prendere atto della selezione operata dal costituente con riferimento a quei valori che, come l'esperienza storica si è incaricata di dimostrare, hanno manifestato una maggiore suscettibilità di fronte all'esercizio, talora arbitrario, dei pubblici poteri»[555], con la conseguenza che la mera compressione del diritto alla privacy, svincolata da un contesto domiciliare o comunicativo, non comporta alcuna ipotesi di prova incostituzionale.

Tuttavia, e siamo al secondo profilo oggetto di interesse, la localizzazione satellitare presuppone un'attività materiale di intrusione all'interno dell'autovettura del soggetto da monitorare al fine di installare furtivamente la stazione ricevente il segnale *gps* proveniente dai satelliti[556]. Ebbene, secondo una prima ricostruzione, di matrice dottrinaria, l'abitacolo di un autoveicolo rientra tra i luoghi protetti dall'art. 14 Cost., in quanto si tratta pur sempre di un ambito spaziale isolato rispetto all'esterno, destinato allo svolgimento di attività inerenti la vita privata e caratterizzato da uno *ius excludendi alios* in capo al titolare del mezzo[557]. Con questa premessa, la conclusione è scontata: la legittimità dell'intervento intrusivo finalizzato alla predisposizione del ricevitore *gps* necessita di una previsione legislativa in ordine ai "casi e ai modi" in cui può avvenire e di un previo atto motivato dell'autorità giudiziaria. La tesi che prevale in giurisprudenza, tuttavia, è di segno opposto e tende ad escludere che l'abitacolo dell'autoveicolo possa qualificarsi come "domicilio" rilevante ai fini dell'art. 14 Cost. In

---

[553] L.G. VELANI, *Nuove tecnologie e prova penale: il sistema di individuazione satellitare g.p.s*, cit., p. 2375, il quale, a ragionar diversamente, avverte anche una potenziale violazione dell'art. 3 Cost., a causa della irragionevole disparità di trattamento tra mezzi di ricerca della prova nominati, per i quali è previsto dal codice di rito il controllo giurisdizionale, e strumenti atipici comunque incidenti, quantomeno, sulla riservatezza.

[554] Così, A. SERRANI, *Sorveglianza satellitare GPS: un'attività investigativa ancora in cerca di garanzie*, in *Arch. pen.*, 2013, 3, che richiama Corte eur. dir. uomo, 9 maggio 2003, Papageorgiou c. Grecia, in

[555] Così, C. MARINELLI, *Intercettazioni processuali*, cit., p. 247.

[556] Tecnicamente, tale intrusione può essere fatta in due modi: intervenendo dall'esterno e collocando il dispositivo direttamente alla batteria contenuta nel vano motore del veicolo; inserendo la ricevente all'interno dell'abitacolo, opportunamente occultata, onde evitare il rischio di essere scoperti.

[557] Cfr. G. BORRELLI, *Riprese filmate*, cit., p. 2453; C. BOTTI, *Ma il sensore posto nell'autoveicolo potrebbe violare il domicilio*, cit., p. 17, secondo il quale «una intrusione ad opera degli organi investigativi [dovrebbe] essere legittimata e giustificata solo in casi e in ipotesi specifiche, con modalità individuate, attraverso l'applicazione, per analogia, della disciplina prevista per le intercettazioni ambientali e telefoniche, trovandosi di fronte a situazioni riferibili alla stessa ratio normativa»; C. FANUELE, *Il concetto di privata dimora ai fini delle intercettazioni ambientali*, in *Cass. pen.*, 2001, p. 2746.

quanto mezzo di trasporto, si sostiene, l'autovettura difetta di quelle caratteristiche tipiche dei luoghi di privata dimora che consentono l'espletamento, in condizioni di riservatezza, delle più elementari funzioni umane[558]. Di conseguenza, l'attività intrusiva finalizzata alla mera installazione del dispositivo di controllo non necessita di alcuna legge di copertura né comporta la previa autorizzazione dell'autorità giudiziaria.

Ciò detto, senza voler prendere posizione a favore dell'una o dell'altra opinione, la soluzione migliore sarebbe, *de iure condendo*, l'introduzione di una disciplina specifica idonea a realizzare un equo bilanciamento tra esigenze dell'accertamento penale e diritti individuali coinvolti in tale accertamento. Infatti, alla luce di un progresso tecnologico foriero di mezzi di indagine sempre più penetranti e invasivi, la supplenza giurisdizionale può diventare rischiosa. Ed allora, anche con riferimento al rilevamento mediante *g.p.s.* sarebbe opportuno un intervento legislativo che si occupasse di specificare le tipologie di reato per le quali consentire il monitoraggio, le modalità preparatorie ed esecutive, la riserva di giurisdizione, la forma della documentazione delle operazioni, le sanzioni processuali in ipotesi di violazione dei presupposti legittimanti l'uso dello strumento investigativo[559].

---

[558] Cfr. Cass., sez. un., 31 ottobre 2001, Policastro, in *Foro it.*, 2002, II, c. 170; Cass., sez. VI, 1 dicembre 2003, in *Cass. pen.*, 2005, p. 1995; Cass., sez. II, 4 maggio 2001, Berlingieri, in *Arch. giur. circ.*, 2001, p. 818; Cass., sez. VI, 23 gennaio 2001, De Palma, *ivi*, p. 2751; Cass., sez. I, 18 ottobre 2000, Galli, in *Cass. pen.*, 2001, p. 2746; Cass., sez. I, 22 gennaio 1996, Porcaro, *ivi*, p. 1082; Cass., sez. I, 27 gennaio 1987, Catanzaro, *ivi*, 1988, p. 916; Cass., sez. I, 19 febbraio 1981, Semitaio, in *Giust. pen.*, 1982, II, c. 73. Di segno contrario, tuttavia, si segnala Cass., sez. II, 12 marzo 1988, Zagaria, in *Riv. pen.*, 1988, p. 1177. In dottrina, a favore della impossibilità di ricondurre l'abitacolo dell'autoveicolo al concetto di domicilio, cfr. P. GIORDANO, *Inapplicabili le garanzie dell'intercettazione al semplice monitoraggio della posizione*, in *Guida dir.*, 2002, 23, p. 54, secondo il quale esiste una ontologica ed insuperabile differenza tra un mezzo di trasporto e una privata dimora, poiché quest'ultima «echeggia una struttura abitativa stabile tendenzialmente immobiliare».

[559] Di questo avviso, fra gli altri, L. FILIPPI, *Il GPS è una prova "incostituzionale"? Domanda provocatoria, ma non troppo, dopo la sentenza Jones della Corte Suprema U.S.A.*, in *Arch. pen.*, 2012, p. 1.

CAPITOLO 6
DATA RETENTION

Sommario: 1. Premessa - 2. La decisione della Corte di giustizia e l'accertamento della violazione della Carta dei diritti fondamentali - 3. Il destino dell'art. 132 del Codice della privacy - 4. Il *freezing* dei dati.

1. Premessa

Per *data retention* si intende la conservazione, effettuata da parte dei c.d. gestori di servizi di connettività, dei dati relativi al traffico telefonico e telematico effettuato dall'utente. Dietro formale richiesta, tali dati devono essere forniti all'autorità procedente che se ne serve per fini di accertamento e repressione dei reati. La fonte normativa di riferimento, come noto, è la direttiva 2006/24/CE[560], recepita in attraverso la modifica dell'art. 132 del Codice della privacy[561].

I dati memorizzati dal gestore per obbligo di legge, diversi a seconda che si parli di telefonia fissa, telefonia mobile o rete Internet, servono ai seguenti scopi: rintracciare e identificare la fonte[562] e la destinazione[563] di una comunicazione telefonica e/o telematica;

---

[560] 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, accessibile *on line* al seguente url: www.garanteprivacy.it.

[561] Come noto, si tratta del D. Lgs. 30 giugno 2003, n. 196 (G.U. 29 luglio 2003), il cui art. 132 (Conservazione di dati di traffico per altre finalità) è stato modificato inizialmente dal decreto-legge 24 dicembre 2003, n. 354, convertito con modificazioni dalla legge di conversione 26 febbraio 2004, n. 45, recante interventi per l'amministrazione della giustizia; poi dal decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge di conversione 31 luglio 2005, n. 155, recante misure urgenti per il contrasto del terrorismo internazionale; successivamente, dalla legge 18 marzo 2008, n. 48, recante ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno; e, da ultimo, dal decreto legislativo 30 maggio 2008, n. 109, di attuazione della direttiva 2006/24/Ce riguardante la conservazione dei 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.

[562] In particolare, per la telefonia di rete fissa e la telefonia mobile i dati necessari per rintracciare e identificare la fonte di una comunicazione sono il numero telefonico chiamante, il nome e l'indirizzo dell'abbonato o dell'utente registrato. Per quanto riguarda l'accesso ad Internet, la posta elettronica e la comunicazione via Internet, invece, il gestore deve memorizzare l'identificativo/i dell'utente, il numero telefonico assegnati a ogni comunicazione sulla rete telefonica pubblica, il nome e l'indirizzo dell'abbonato o dell'utente regi-strato a cui al momento della comunicazione sono stati assegnati l'indirizzo di protocollo Internet (IP), un identificativo di utente o un numero telefonico.

determinare la data, l'ora e la durata di una comunicazione telefonica o di una connessione ad Internet[564]; determinare il tipo di comunicazione e/o connessione[565]; determinare le attrezzature di comunicazione degli utenti[566]; determinare l'ubicazione delle apparecchiature di comunicazione mobile[567]. Ovviamente, nessun dato relativo al contenuto di una comunicazione, comunque essa venga fatta, può essere conservato a norma della direttiva sulla c.d. *data retention*[568].

L'accesso a questa enorme mole di dati spetta esclusivamente «alle autorità nazionali competenti, in casi specifici e conformemente alle normative nazionali. Le procedure da seguire e le condizioni da rispettare per avere accesso ai dati conservati in conformità dei criteri di necessità e di proporzionalità sono definite da ogni Stato membro nella legislazione nazionale, con riserva delle disposizioni in materia del diritto dell'Unione europea o del diritto pubblico internazionale e in particolare della CEDU, secondo l'interpretazione della Corte europea dei diritti dell'uomo»[569].

---

[563] Quanto ai dati necessari per rintracciare e identificare la destinazione di una comunicazione: per la telefonia di rete fissa e la telefonia mobile, numero/i digitato/i (il numero o i numeri chiamati) e, nei casi che comportano servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero o i numeri a cui la chiamata è trasmessa, nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i; per la posta elettronica su Internet e la telefonia via Internet, identificativo dell'utente o numero telefonico del/dei presunto/i destinatario/i di una chiamata telefonica via Internet, nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i e identificativo del presunto destinatario della comunicazione.

[564] Quanto ai dati necessari per determinare la data, l'ora e la durata di una comunicazione, per la telefonia di rete fissa e la telefonia mobile, essi consistono nella data e nell'ora dell'inizio e della fine della comunicazione; per l'accesso Internet, la posta elettronica via Internet e la telefonia via Internet: 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; data e ora del log-in e del log-off del servizio di posta elettronica su Internet o del servizio di telefonia via Internet sulla base di un determinato fuso orario.

[565] I dati necessari per determinare il tipo di comunicazione sono: per la telefonia di rete fissa e la telefonia mobile, il servizio telefonico utilizzato; per la posta elettronica Internet e la telefonia Internet, il servizio Internet utilizzato.

[566] I dati necessari per determinare le attrezzature di comunicazione degli utenti sono i seguenti: per la telefonia di rete fissa, numeri telefonici chiamanti e chiamati; per la telefonia mobile, numeri telefonici chiamanti e chiamati; International Mobile Subscriber Identity (IMSI) del chiamante; International Mobile Equipment Identity (IMEI) del chiamante; l'IMSI del chiamato; l'IMEI del chiamato; nel caso dei servizi prepagati anonimi, la data e l'ora dell'attivazione iniziale della carta e l'etichetta di ubicazione (Cell ID) dalla quale è stata effettuata l'attivazione; per l'accesso Internet, la posta elettronica su Internet e la telefonia via Internet: numero telefonico chiamante per l'accesso commu- tato (dial-up access); digital subscriber line (DSL) o un altro identificatore finale di chi è all'origine della comunicazione.

[567] Infine, i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile: etichetta di ubicazione (Cell ID) all'inizio della comunicazione; 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.

[568] Cfr. par. 5, co. 2, Direttiva 2006/24/CE.

[569] Così, il par. 4 della Direttiva 2006/24/CE.

La normativa in materia è rappresentata dal c.d. Codice della privacy, il cui art. 132, modificato proprio allo scopo di recepire le indicazioni provenienti dalla fonte europea, prevede le modalità operative della c.d. *data retention*. In particolare: «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»[570]. Entro tali termini, «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»[571]. Quindi, lo strumento processuale per acquisire processualmente tali informazioni è rappresentato dall'art. 256 c.p.p., da leggere in combinato disposto con l'art. 132, co. 1 e 3, del d. lgs. n. 196 del 2003.

Non vi è alcun dubbio che la conservazione dei dati di traffico telefonico e telematico (c.d. dati esterni di una comunicazione) effettuata dai gestori a prescindere dall'esistenza di un procedimento penale pendente faciliti il lavoro investigativo e di intelligence degli inquirenti. Le informazioni potenzialmente ottenibili *ex post* grazie a tale preventiva opera di memorizzazione rappresentano uno strumento imprescindibile per la prevenzione e la repressione dei reati. In particolare, con specifico riferimento al traffico telematico, grazie alla "collaborazione" degli Internet *Service Providers*, gli investigatori sono in grado non soltanto di identificare un determinato soggetto utente della Rete[572], ma anche di ricostruirne l'attività *online*[573]. E' ovvio che quando l'attività investigativa riguarda illeciti commessi in Rete da soggetti non identificati (pedopornografia *online*, truffe telematiche, diffamazione *online*, ecc.) questo tipo di informazioni rappresenta il primo indispensabile tassello di una successiva attività di indagine finalizzata ad accertare i fatti. Evidentemente, la mancanza di questi dati digitali, la cui acquisizione è propedeutica rispetto ad ogni altro adempimento, comprometterebbe qualsiasi successiva azione investigativa. Se possibile, l'importanza del *data retention* cresce ancor di più con riferimento a quell'attività di intelligence, di *ratio*

---

[570] Art. 132, co. 1, Codice della privacy.
[571] Art. 132, co. 3, Codice della privacy.
[572] Attraverso il c.d. indirizzo IP, ossia «un numero che identifica un dispositivo collegato a una rete telematica: esso piò essere paragonato a un indirizzo stradale o a un numero telefonico. Il fornitore di connettività, infatti, dato un indirizzo IP e l'ora di accesso a tale indirizzo, è in grado di fornire i dati personali di chi ha sottoscritto il contratto per usufruire dei servizi di connessione». G. VACIAGO, *Profili processuali delle indagini informatiche*, cit., p. 645.
[573] Tramite il c.d. *file* di *log*, ossia «un file in cui sono memorizzate le attività compiute da un determinato utente […] all'interno del computer o in Rete». *Ibidem*.

preventiva, che caratterizza l'operato dei servizi di informazione per la sicurezza della Repubblica.

Tuttavia, esiste una relazione di diretta proporzionalità fra conservazione dei dati digitali e rischio di lesione di alcuni diritti fondamentali degli utenti del *web*, primo fra tutti il diritto alla privacy. Esiste, cioè, una evidente frizione tra le esigenze di prevenzione e di accertamento dei reati e la necessità di tutelare la riservatezza di coloro i quali utilizzano la Rete per gli scopi più disparati, ma anche leciti. In particolare, l'attività di *data retention* costituisce una limitazione del diritto al rispetto della vita privata e di quello alla tutela dei dati personali, garantiti rispettivamente dagli artt. 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea. Infatti, pur non consentendo di apprendere il contenuto di una comunicazione, i dati digitali esterni forniscono informazioni sulla vita privata di una persona e possono essere utilizzati per creare veri e propri profili della personalità, in quanto consentono di tracciare i movimenti degli utenti, «ingenerando nei cittadini l'impressione di vivere in una società del controllo di orwelliana memoria: destinatario, data, luogo, orario di una comunicazione, siti Internet visitati permettono, se combinati tra loro, e se la conservazione riguarda un lasso di tempo apprezzabile, di ottenere dettagliate informazioni ad esempio sugli orientamenti religiosi, sull'appartenenza a gruppi politici o associazioni sindacali, sulle relazioni sociali o sulle inclinazioni personali, costituendo senza dubbio un'ingerenza nel diritto alla riservatezza della vita privata»[574].

Ancora una volta è necessario un compromesso, un equilibrio tra opposte esigenze, entrambe meritevoli di accoglimento. Ebbene, i pilastri del bilanciamento sono elencati nell'art. 52, comma 1, della Carta dei Diritti Fondamentali dell'Unione Europea, secondo cui l'ingerenza "pubblica" nella "vita privata" deve essere prevista dalla legge, deve rispettare il nucleo essenziale dei diritti coinvolti e deve essere proporzionata all'obiettivo da raggiungere, corrispondente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

[574] Così, F. IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, in *Cass. pen.*, 12, 2014, p. 4274, la quale richiama in nota 1) la sentenza del BVerfG, 2 marzo 2010, 1BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, reperibile anche su www.bundesverfassungsgericht.de.

2. La decisione della Corte di giustizia e l'accertamento della violazione della Carta dei diritti fondamentali

La Corte di giustizia dell'Unione europea, con le decisioni riunite C-293/12 e C-594/12 dell'8 aprile 2014[575], ha dichiarato invalida la direttiva 2006/24/CE sul *data retention*. Il percorso motivazionale della sentenza della Corte si snoda attraverso i seguenti fondamentali passaggi logici.

Innanzitutto, la Corte segnala che, sebbene dall'art. 1 e dall'art. 5 della direttiva si evinca chiaramente il divieto di custodire il contenuto delle conversazioni avvenute attraverso i canali elettronici, i dati sottoposti all'obbligo di conservazione (mittente e destinatario della comunicazione, durata e tipo di comunicazione, nome e indirizzo dell'utilizzatore, numero chiamante e numero chiamato, indirizzo IP, localizzazione del chiamante e apparecchiature utilizzate) permettono di tracciare profili piuttosto definiti riguardo alle persone che utilizzano i mezzi di comunicazione. Pertanto, a giudizio della Corte, la verifica della legittimità di una simile operazione chiama direttamente in causa l'art. 7, l'art. 8 e l'art. 11 della Carta dei diritti fondamentali dell'Unione europea perché la pratica della conservazione dei dati può, con tutta

---

[575] C. Giust. UE, 8 aprile 2014, cause riunite C-293/12, C-594/12. Per un primo commento della sentenza, v. COLOMBO, *"Data retention" e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen.*, 2014, 7/8, p. 2705, nonché R. FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, www.penalecontemporaneo.it, 30 novembre 2015. La vicenda giudiziaria in questione trae origine da due distinte controversie giudiziarie nazionali che in ragione del loro comune oggetto sono state processualmente riunificate e hanno portato ad un'unica risposta della Corte europea. In primo luogo, è stata la Corte suprema irlandese che, per risolvere un caso in cui una ONG contestava la direttiva e l'atto nazionale di recepimento, ha sollevato una serie di questioni pregiudiziali e ha chiesto al giudice del Lussemburgo di verificare se la disciplina europea abbia compiuto un bilanciamento adeguato tra la necessità di garantire la sicurezza e il corretto funzionamento del mercato interno e la necessità di garantire la libertà di circolazione (come tutelata dall'art. 21 del Trattato sul funzionamento dell'Unione europea), il rispetto della vita privata (come tutelato dall'art. 7 della Carta europea dei diritti fondamentali e dall'art. 8 della Convenzione europea), la protezione dei dati personali (come tutelata dall'art. 8 della Carta europea dei diritti fondamentali), la libertà di espressione (come tutelata dall'art. 11 della Carta europea dei diritti fondamentali e dall'art. 10 della Convenzione europea) e il diritto ad una buona amministrazione (come tutelato dall'art. 41 della Carta europea dei diritti fondamentali). La stessa Corte irlandese ha poi richiesto in che misura il principio di leale collaborazione imponga al giudice nazionale di valutare in autonomia la compatibilità tra i diritti e le libertà affermati dalla Carta europea dei diritti fondamentali (interpretate alla luce della Convenzione) e le norme nazionali di attuazione dei provvedimenti di origine sovranazionale. In secondo luogo, è stata la Corte costituzionale austriaca che, per rispondere ai ricorsi con cui il governo della Carinzia e 11.130 privati cittadini hanno richiesto l'annullamento della legge interna di recepimento della direttiva, ha a sua volta chiesto se il sistema di raccolta dei dati sia compatibile con il diritto al rispetto della vita privata, con il diritto alla protezione dei dati personali e con il diritto alla libertà di espressione tutelati dalla Carta dei diritti fondamentali. Inoltre, la stessa istituzione giudiziaria austriaca ha domandato alcuni chiarimenti in merito al significato delle clausole orizzontali e, in particolare, ha chiesto alla Corte del Lussemburgo di verificare se il quadro normativo europeo rispetti il contenuto essenziale del diritto alla protezione dei dati personali, se le limitazioni imposte siano conformi al principio della protezione dei dati personali e se la conservazione dei dati sia compatibile con le tradizioni costituzionali comuni e con l'art. 8 della Convenzione europea.

evidenza, interferire con la libertà di espressione, con la riservatezza della vita privata e con la protezione dei dati personali[576].

Una volta accertata la portata dell'ingerenza, la Corte ne vaglia la legittimità ai sensi delle regole generali dell'ordinamento europeo. A questo proposito, i giudici si richiamano alle prescrizioni contenute nel già citato art. 52 della Carta: 1) tutela del nucleo essenziale dei diritti coinvolti; 2) finalità legittima dell'ingerenza; 3) proporzionalità e stretta necessità della misura.

Quanto al primo requisito, la Corte esclude che la normativa europea sul *data retention* sia in qualche modo in grado di intaccare il nucleo essenziale dei diritti coinvolti: quanto all'art. 7, «poiché, come deriva dall'articolo 1, paragrafo 2, della stessa direttiva, quest'ultima non permette di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tale»[577]; quanto all'art. 8, poiché «i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione sono tenuti a rispettare taluni principi di protezione e di sicurezza dei dati, principi in base ai quali gli Stati membri assicurano l'adozione di adeguate misure tecniche e organizzative contro la distruzione accidentale o illecita, la perdita o l'alterazione accidentale dei dati»[578].

Inoltre, secondo la Corte è fuori discussione che «la conservazione dei dati per permettere alle autorità nazionali competenti di disporre di un accesso eventuale agli stessi, come imposto dalla direttiva 2006/24, risponde effettivamente a un obiettivo di interesse generale»[579]: i dati digitali «costituiscono uno strumento particolarmente importante e valido nella prevenzione dei reati e nella lotta contro la criminalità, in particolare della criminalità organizzata»[580].

Il *punctum dolens* è rappresentato dalla proporzionalità e dalla stretta necessità dell'ingerenza. In base all'interpretazione offerta dalla Corte europea, una normativa in tema di *data retention* può dirsi rispettosa del principio di proporzionalità se: 1) individua dei limiti di natura temporale, spaziale, soggettiva o oggettiva alla conservazione; 2) stabilisce criteri oggettivi finalizzati a disciplinare l'accesso e l'utilizzo da parte delle competenti autorità

---

[576] La Corte constata che «l'ingerenza che la direttiva 2006/24 comporta nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta si rivela essere […] di vasta portata e va considerata particolarmente grave» e aggiunge che «la conservazione dei dati e l'utilizzo ulteriore degli stessi […] effettuati senza che l'abbonato o l'utente registrato ne siano informati può ingenerare nelle persone interessate […] la sensazione che la loro vita privata sia oggetto di costante sorveglianza». Cfr. C. Giust. UE, 8 aprile 2014, cit., par. 37.
[577] *Ivi*, par. 39.
[578] *Ivi*, par. 40.
[579] *Ivi*, par. 44.
[580] *Ivi*, par. 43.

nazionali (per fini di prevenzione o repressione di reati considerati sufficientemente grafi da giustificare siffatta ingerenza) dei dati raccolti; 3) prevede modalità sostanziali e procedurali per l'accesso ai dati da parte delle autorità competenti che, comunque, non possono prescindere da un vaglio preventivo ad opera di un giudice o di un'entità amministrativa indipendente che limiti l'accesso e l'acquisizione a quanto strettamente necessario a raggiungere l'obiettivo perseguito; 4) distingue la durata della conservazione a seconda dell'obiettivo perseguito o della persona interessata; 5) fissa criteri obiettivi che garantiscano che la conservazione sia limitata a quanto strettamente necessario; 6) predispone sufficienti misure per garantire la sicurezza e la protezione dei dati, in modo tale da prevenire eventuali accessi abusivi e usi illeciti delle informazioni[581]. Ebbene, secondo la Corte la vaghezza dei criteri utilizzati per definire in maniera oggettiva quali crimini perseguire attraverso i dati conservati, così come l'insufficienza delle condizioni e delle procedure previste per evitare che attraverso la raccolta si possano perpetrare abusi (in particolare, il non aver previsto che l'accesso ai dati possa avvenire in seguito ad un apposito provvedimento dell'autorità giudiziaria), l'assenza di un catalogo di situazioni eccezionali escluse dall'obbligo di conservazione, la mancanza di norme che specificamente garantiscano modalità sicure di trattamento di ingenti quantità di dati (in particolare, la distruzione irreversibile dei dati raccolti) e soprattutto la scelta di un monitoraggio che coinvolge indiscriminatamente tutti i soggetti, tutti i mezzi di comunicazione elettronica e tutti i tipi di dati determinano un quadro normativo che si colloca al di là di quanto strettamente indispensabile per conseguire l'obiettivo della lotta al crimine e al terrorismo[582]. In altre parole, prevedere, da parte del legislatore europeo, obblighi di conservazione indiscriminati dei dati di traffico dell'intera popolazione significa eccedere i limiti imposti dal necessario rispetto del principio di proporzionalità e di stretta necessità della misura invasiva.

---

[581] Ed infatti, i fornitori di servizi di telecomunicazione sono imprenditori e seguiranno verosimilmente criteri di economia, non necessariamente sintomo di alti standards di sicurezza. Così, F. IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, cit., la quale sottolinea come proprio il fatto che i costi della conservazione siano a carico dei fornitori di servizi ha determinato il successo di tale strumento di indagine che per gli investigatori, e quindi per lo Stato, è molto più economico delle intercettazioni. V. ZÖLLER, *Die Vorratsspeicherung von Telekommunikationsdaten – (Deutschen) Wege und Irrwege, Congress on the Criminal Law Reforms* in *The World and in Turkey*, Atti del convegno internazionale svoltosi a Istanbul-Ankara dal 26 maggio al 4 giugno 2010, Istanbul, 2010, p. 33.

[582] «La normativa dell'Unione […] deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati. La necessità di disporre di siffatte garanzie è tanto più importante allorché, come prevede la direttiva 2006/24, i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi». *Ivi*, par. 54.

Quindi, «adottando la direttiva 2006/24, il legislatore dell'Unione ha ecceduto i limiti imposti dal rispetto del principio di proporzionalità alla luce degli articoli 7, 8 e 52, paragrafo 1, della Carta»[583]. Per questo motivo, la Corte (Grande Sezione) ha dichiarato che tale direttiva è invalida.

3. Il destino dell'art. 132 del Codice della privacy

La pronuncia appena citata solleva inevitabilmente questioni applicative di non poco conto con riferimento alla tenuta ed alla sorte della normativa nazionale di attuazione del c.d. *data retention*.

Un dato è certo: l'art. 132 del nostro Codice della privacy non può certo definirsi rispettoso del principio di proporzionalità, così come interpretato dalla Corte europea. Tale norma, infatti: 1) eccezion fatta per il fattore tempo, non pone alcun limite alla conservazione dei dati di traffico telefonico e telematico, che risulta quindi indiscriminata[584]; 2) non prevede un elenco di reati particolarmente gravi e tali da giustificare l'ingerenza nella vita privata e nella riservatezza delle persona che è inevitabilmente provocata dal *data retention*[585]; 3) non prevede specifiche modalità procedurali che devono essere osservate per l'accesso ai dati, né richiede il vaglio di un giudice o di altra autorità indipendente[586]; 4) non distingue la durata

---

[583] *Ivi*, par. 69. Tale conclusione viene raggiunta senza neanche il bisogno di prendere in considerazione gli altri problemi sollevati dai rinvii pregiudiziali dei giudici nazionali (in particolare quelli relativi alle possibili lesioni della libertà di espressione).

[584] Le categorie di dati da conservare sono elencate dall'art. 3 d.lg. n. 109/2008, di attuazione della direttiva 2006/24/CE.

[585] È infatti semplicemente prescritto che i dati vengano conservati «per finalità di accertamento e repressione di reati».

[586] Come già chiarito, i dati possono essere acquisiti presso il fornitore «con decreto del pubblico ministero anche su istanza o del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private». Con riferimento a questo aspetto, si condividono pienamente le osservazioni fatte da F. IOVENE, *Data retention*, cit., secondo la quale «nonostante la particolare posizione ricoperta dal pubblico ministero nel nostro ordinamento, non pare che il suo intervento nella procedura acquisitiva soddisfi i requisiti pretesi dalla Corte di giustizia. Questa, infatti, nel fare riferimento ad un giudice o altra entità indipendente esige che sull'accesso da parte delle autorità a ciò autorizzate vigili un soggetto in posizione di terzietà, quale non è il pubblico ministero, pur sempre parte, ancorché pubblica. Occorrerebbe quindi ricorrere al classico schema che il codice di rito richiede per misure fortemente limitative dei diritti fondamentali: richiesta del pubblico ministero – autorizzazione del giudice, salvo nei casi di urgenza la possibilità per il primo di intervenire autonomamente, con successiva convalida». Di questo avviso anche R. FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, www.penalecontemporaneo.it, 30 novembre 2015, il quale osserva acutamente che, nella sua versione originaria, l'art. 132 codice privacy prevedeva che l'acquisizione dei dati fosse di competenza del giudice.

della conservazione in base al fine perseguito o al soggetto attenzionato[587]; 5) non prevede misure per la sicurezza dei dati[588].

Quale, dunque, la sorte della normativa nazionale alla luce del *decisum* della Corte europea? Il quesito proposto è tutt'altro che semplice da evadere: ed infatti, se da un lato non ci sono dubbi sul fatto che la dichiarazione di invalidità pronunciata dalla Corte valga a sanare la posizione di quelle Nazioni che non hanno ancora provveduto a recepire la direttiva, semplificandone la posizione, dall'altro lato le cose si complicano in quei Paesi, come l'Italia, che hanno dato attuazione all'atto normativo europeo. Ciò in quanto, almeno formalmente, in tali paesi restano in vigore i provvedimenti nazionali di recepimento e in ossequio alle regole sulla competenza previste nei trattati istitutivi, l'intervento normativo europeo preclude la possibilità di un ulteriore intervento legislativo nazionale diverso da quello di attuazione. A ciò si aggiunga che, in ragione dei tempi decisionali piuttosto lunghi, difficilmente si potrà sperare in una soluzione legislativa di fonte sovranazionale che adegui il quadro europeo ai dettami della sentenza. Così, se vi possono essere ben pochi dubbi sul fatto che i giudici irlandesi e austriaci provvederanno presto a bloccare l'efficacia delle rispettive normative interne e a riordinare il quadro normativo e che anche la Corte costituzionale slovena (che, in attesa della pronuncia del giudice europeo sulla validità della direttiva, aveva sospeso il procedimento di controllo di costituzionalità dell'atto interno) arriverà ad una celere definizione della questione, probabilmente in tutti gli altri paesi membri ci si troverà di fronte ad una grave situazione di incertezza giuridica.

Diverse ed alternative le possibili soluzioni. Di primo acchito, in virtù della primazia e dell'effetto diretto del diritto primario europeo, si potrebbe essere indotti a sostenere l'obbligo per il giudice nazionale di disapplicare l'art. 132 del Codice della privacy, in quanto limitativo del diritto al rispetto della vita privata e del diritto alla tutela dei propri dati personali (artt. 7 e 8 CDFUE) oltre quanto strettamente necessario alla luce del principio di proporzionalità (art. 52 CDFUE). Dal punto di vista processuale, da tale disapplicazione dovrebbe conseguire una

---

[587] Semplicemente, distingue tra dati relativi al traffico telefonico, a quello telematico e alle chiamate senza risposta che devono essere conservati rispettivamente per ventiquattro mesi, dodici mesi e trenta giorni.

[588] Ed infatti, il co. 5 dell'art. 132 prescrive che i dati vengano «conservati con accorgimenti ["tecnologici"] volti a garantire i medesimi requisiti di qualità, sicurezza e protezione dei dati in rete, nonché a: a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento [...] d) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui al comma 1». La concreta individuazione di tali standards, tuttavia, è lasciata ai singoli fornitori di servizi, che verosimilmente prediligeranno criteri di economicità ad elevate garanzie per la sicurezza.

inutilizzabilità *ex* art. 191 c.p.p. dei dati eventualmente acquisiti[589]. Ciò in quanto il rilevato contrasto tra la pratica della conservazione dei dati e i diritti tutelati dall'ordine giuridico europeo si dovrebbe riflettere anche sulle norme nazionali di attuazione, opportunamente conducendo alla non applicazione del diritto interno contrastante con la Carta[590].

In base ad altra ricostruzione, stante la problematicità di sanzionare con la non applicazione il contrasto tra la Carta e le norme interne esplicitamente finalizzate a darle attuazione, gli unici rimedi che residuano per risolvere tale contrasto sono quelli predisposti dal diritto nazionale. Con specifico riferimento all'ordinamento italiano (come per tutti gli altri sistemi europei che non hanno un controllo diffuso di costituzionalità) ciò significa che il giudice dovrebbe investire la Corte costituzionale per la declaratoria di incostituzionalità dell'art. 132 del Codice della privacy per contrasto con l'art. 117 della Costituzione, così come integrato dall'art. 7 e dall'art. 8 della Carta europea. Sebbene una simile soluzione sia certamente conforme alle logiche che secondo la giurisprudenza costituzionale italiana presidiano il tema della relazione tra gli ordinamenti, essa ha però il limite della problematica situazione di incertezza giuridica perdurante per tutta la durata della procedura di annullamento.

Ed allora, occorre ragionare diversamente. A ben guardare, la direttiva sulla conservazione dei dati è stata espressamente concepita come una deroga alle norme che in ambito europeo regolano il trattamento dei dati personali e la tutela della privacy e che in generale prevedono per gli operatori economici l'espresso obbligo di distruggere i dati raccolti nell'esercizio delle loro attività. Se si adotta questa prospettiva, una volta che la pratica del *data retention* non può più godere della copertura offerta in via derogatoria dalle norme della direttiva 2006/24/CE, sarebbe necessario ridare piena applicazione alla disciplina generale, concludendo per la disapplicazione delle norme interne (e dell'art. 132 del Codice della privacy in particolare) che prevedono l'obbligo di conservazione dei dati poiché in contrasto con le regole europee che disciplinano questo ambito. Una simile soluzione avrebbe innanzitutto il vantaggio della tempistica: essendo già stata acclarata dalla Corte di giustizia l'illegittimità della pratica della conservazione, il giudice ordinario potrebbe procedere

---

[589] Di questa opinione, tra gli altri, F IOVENE, *Data retention*, cit., nonché S. MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, cit., p. 2855

[590] Il ricorso ad una simile soluzione sembrerebbe addirittura incoraggiato dalla giurisprudenza (si vedano le decisioni Åkerberg, Siragusa e Pelckmans) con cui la Corte di giustizia ha interpretato estensivamente la clausola in questione fino ad escludere la possibilità che la norma si riferisca esclusivamente agli atti interni formalmente vincolati all'ordine giuridico europeo e fino a far coincidere il concetto di attuazione con l'adozione di un qualunque provvedimento adottato in ambiti materiali di competenza dell'Unione.

all'immediata disapplicazione dell'art. 132 senza doversi preoccupare di rinviare la questione ad altra istanza giudiziaria. Per di più, essendo già stato definito il regime alternativo a quello disposto dalle norme interne, verrebbero meno i rischi di un intervento creativo delle istituzioni giudiziarie ordinarie, perché, in ultima analisi, si tratterebbe di dare applicazione alle regole generali sul trattamento dei dati.

Sullo sfondo rimangono problematiche tutt'altro che irrilevanti. Innanzitutto, la disapplicazione dell'art. 132 del Codice della privacy rappresenta un rimedio legato al caso concreto, destinato ad operare *ex post*, che non risolve la violazione dei diritti fondamentali connessa alla mera conservazione dei dati, a prescindere dalla loro successiva ed eventuale acquisizione per fini di giustizia[591]. Forti della declaratoria di invalidità della direttiva, potrebbe essere persino ipotizzato l'obbligo, per i *service providers*, di astenersi dal conservare i dati di traffico, oppure la possibilità per i privati di chiedere, ai sensi dell'art. 7, comma 3, lett. b) codice privacy, la cancellazione dei dati che li riguardano in quanto illecitamente trattati.

Inoltre, rimane aperto lo spinoso tema della prevenzione: la conservazione e l'acquisizione dei dati per finalità di *intelligence*[592] sfuggono alla soluzione della disapplicazione, non potendo fisiologicamente tali dati essere utilizzati in un eventuale instaurando processo penale[593].

4. Il *freezing* dei dati

Diverso dal *data retention* è l'affine istituto del c.d. *freezing* dei dati di cui ai commi 4-*ter*, 4-*quater* e 4-*quinquies* dell'art. 132 del d. lgs. n. 196 del 2003, così come introdotti dall'art. 10 della legge n. 48 del 2008. In sintesi, la normativa sul c.d. congelamento dei dati prevede: a) l'obbligo, gravante sui *service providers*, di conservazione dei dati di traffico telematico per un periodo di novanta giorni prorogabile fino a sei mesi, su richiesta dei soggetti indicati

---

[591] Il sistema del *data retention* comporta due distinte intromissioni nella vita privata: la prima si verifica in ogni caso per effetto della "semplice" conservazione, la seconda, successiva ed eventuale, si ha al momento della acquisizione dei dati per finalità di prevenzione o di repressione di reati.

[592] Questa diversa ipotesi è disciplinata, sempre in attuazione della direttiva europea, dal comma 4-*ter* dell'art. 132 codice privacy.

[593] L'art. 132, comma 4-*ter*, codice privacy fa testuale riferimento allo «svolgimento delle investigazioni preventive previste dal citato art. 226 delle norme di cui al decreto legislativo n. 271 del 1989», norma che sancisce espressamente un divieto di utilizzazione degli elementi acquisiti attraverso le attività preventive nel processo penale, fatti salvi i fini investigativi.

al comma 4-*ter*[594], per finalità di indagine essenzialmente preventiva, ovvero per finalità di accertamento e repressione di specifici reati; b) l'applicabilità, nei confronti del *service provider*, dell'art. 326 c.p. in ipotesi di rivelazione del segreto connesso all'ordine di conservazione ricevuto; c) la convalida di detto provvedimento entro 48 ore da parte del pubblico ministero.

La differenza tra *data retention e data freezing* è presto detta: la prima attività comporta due distinte intromissioni nella vita privata, la prima delle quali si verifica per effetto della "semplice" conservazione, mentre la seconda, successiva ed eventuale, si realizza al momento della acquisizione dei dati per finalità di prevenzione o di repressione di reati; il *freezing*, invece, implica esclusivamente l'acquisizione dei dati digitali a partire dal momento in cui, per esigenze di giustizia tipizzate nel codice privacy, si abbia una specifica richiesta dell'autorità competente. In altre e più semplici parole, l'attività riconducibile al *data retention* prescinde, almeno nella sua fase preliminare e propedeutica di raccolta dei dati, dalle esigenze investigative, di natura preventiva o repressiva. Viceversa, il *freezing* viene ordinato «ai fini dello svolgimento delle investigazioni preventive […] ovvero per finalità di accertamento e repressione di specifici reati»[595]. Ergo, tale strumento presuppone la preesistenza di quelle esigenze di giustizia che, invece, possono essere solo eventuali in ipotesi di *data retention*.

Rispetto alla conservazione indiscriminata del traffico telematico generato dall'utente (art. 132, co. 1, Codice della privacy), il congelamento urgente di cui ai commi 4-*ter*, 4-*quater* e 4-*quinquies* dell'art. 132 del Codice della privacy rappresenta sicuramente un compromesso migliore tra le esigenze pubblicistiche di giustizia, intese in senso lato, e i diritti individuali degli utenti della Rete. L'equilibrio è maggiore in quanto il *freezing* consente di evitare quella continua sorveglianza e quel continuo monitoraggio che, prescindendo dall'acquisizione di una *notizia criminis* o, quantomeno, da esigenze di natura preventiva, sono in grado di influire, nel medio e lungo periodo, sulla libertà di autodeterminazione della persona[596].

A chi scrive non sfugge, ovviamente, il rovescio della medaglia: dal punto di vista investigativo, il congelamento dei dati potrebbe non essere utile o, comunque, non

---

[594] «[…] 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 […]».

[595] Cfr. co. 4-*ter* dell'art. 132 del Codice della privacy.

[596] Sul punto si rinvia a G. DI PAOLO, *Tecnologie del controllo e prova penale. L'esperienza statunitense e spunti per la comparazione*, cit., p. 252.

sufficientemente utile in tutte le ipotesi in cui si arrivi con ritardo alla individuazione del potenziale indagato. Il vuoto temporale esistente tra il momento in cui il soggetto pone in essere condotte utili ai fini investigativi ed il momento in cui tali condotte vengono qualificate come rilevanti dagli investigatori (sia in chiave preventiva che in chiave repressiva) è irrecuperabile attraverso il *freezing*: l'unica strada percorribile per recuperare *ex post* il terreno perduto si chiama *data retention*.

CAPITOLO 7
LE ALTRE INDAGINI DIGITALI OCCULTE

1. Le operazioni digitali sotto copertura ed il monitoraggio dei siti - 2. *Cloud computing* - 3. Il controllo occulto mediante OSint: natura e limiti di ammissibilità.

1. Le operazioni digitali sotto copertura ed il monitoraggio dei siti.

Quando si parla di "operazioni digitali sotto copertura" il riferimento va, in particolare, all'art. 14, co. 2, della legge 3 agosto 1998, n. 269[597] ed all'art. 9, co. 2, della legge 16 marzo 2006, n. 146[598]. Pur con qualche differenza relativa alla legittimazione soggettiva a svolgere tali tipologie di indagini[599], l'idea di fondo che sta alla base di queste due norme è la

[597] «Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù», pubblicata nella Gazz. Uff. 10 agosto 1998, n. 185. Art. 14 (Attività di contrasto): 2. «Nell'ambito dei compiti di polizia delle telecomunicazioni, definiti con il decreto di cui all'articolo 1, comma 15, della legge 31 luglio 1997, n. 249, l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione svolge, su richiesta dell'autorità giudiziaria, motivata a pena di nullità, le attività occorrenti per il contrasto dei delitti di cui agli articoli 600-*bis*, primo comma, 600-*ter*, commi primo, secondo e terzo , e 600-*quinquies* del codice penale commessi mediante l'impiego di sistemi informatici o mezzi di comunicazione telematica ovvero utilizzando reti di telecomunicazione disponibili al pubblico. A tal fine, il personale addetto può utilizzare indicazioni di copertura, anche per attivare siti nelle reti, realizzare o gestire aree di comunicazione o scambio su reti o sistemi telematici, ovvero per partecipare ad esse. Il predetto personale specializzato effettua con le medesime finalità le attività di cui al comma 1 anche per via telematica».

[598] «Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001», pubblicata nella Gazz. Uff. 11 aprile 2006, n. 85, S.O. Art. 9 (Operazioni sotto copertura): «2. Negli stessi casi previsti dal comma 1 [delitti previsti dagli articoli 473, 474, 629, 630, 644, 648-*bis* e 648-*ter*, nonché nel libro II, titolo XII, capo III, sezione I, del codice penale, ai delitti concernenti armi, munizioni, esplosivi, ai delitti previsti dall'articolo 12, commi 1, 3, 3-*bis* e 3-*ter*, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni, nonché ai delitti previsti dal testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, dall'articolo 260 del decreto legislativo 3 aprile 2006, n. 152, e dall'articolo 3 della legge 20 febbraio 1958, n. 75], gli ufficiali e gli agenti di polizia giudiziaria possono utilizzare documenti, identità o indicazioni di copertura, rilasciati dagli organismi competenti secondo le modalità stabilite dal decreto di cui al comma 5, anche per attivare o entrare in contatto con soggetti e siti nelle reti di comunicazione, informandone il pubblico ministero al più presto e comunque entro le quarantotto ore dall'inizio delle attività» (comma così modificato dalla lettera c) del comma 1 dell'art. 8, L. 13 agosto 2010, n. 136).

[599] Le attività di contrasto in materia di pedopornografia di cui all'art. 14, comma 2, della l. n. 266 del 1998 sono di esclusiva competenza del personale che svolge "compiti di polizia delle comunicazioni"; viceversa, le operazioni sotto copertura di cui parla l'art. 9 della l. n. 146 del 2006 sono attribuite, più in generale, agli ufficiali di polizia giudiziaria appartenenti ai reparti specializzati della Polizia di Stato, dell'Arma dei Carabinieri

medesima: sfruttare le potenzialità investigative del c.d. "agente infiltrato"[600] per contrastare i più gravi delitti commessi attraverso la rete Internet, attraverso la figura dell' "agente provocatore *online*".

Una premessa non appare fuori luogo: in questa particolare figura si sommano vecchie e nuove problematiche, prima fra tutte l'incresciosa circostanza che nella prassi investigativa, sicuramente anche in ragione della manifesta odiosità dei reati in questione, spesso si è assistito ad operazioni sotto copertura la cui "superficialità" ha comportato un'esposizione mediatica estremamente lesiva della riservatezza delle persone sottoposte ad indagine, attesa la stigmatizzazione sociale, difficilmente rimediabile anche attraverso una sentenza di assoluzione. Probabilmente oggi, nell'era dei social network, siamo testimoni di un preoccupante aumento delle distorsioni applicative di una disciplina che, già nel suo tradizionale assetto normativo, presentava non pochi aspetti di elevata criticità in termini di tenuta delle garanzie fondamentali[601].

Attraverso questo tipo di azione investigativa si cerca di interagire *online* con i soggetti sospettati al fine di verificarne e documentarne, a scopo probatorio, eventuali sviluppi criminogeni. Siffatta attività *under cover online* deve essere sorretta dai seguenti elementi indefettibili, che rappresentano altrettanti limiti alla legittimità delle operazioni svolte. Innanzitutto, dal punto vista soggettivo, l'azione investigativa può essere svolta esclusivamente da ufficiali di polizia giudiziaria addetti alla Polizia Postale (organo del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazione) o a strutture specializzate per il contrasto dei delitti di criminalità organizzata. In secondo luogo, è necessario l'intervento dell'autorità giudiziaria, che nel caso di contrasto alla pedopornografia *online*, nonché in ipotesi di delitti di criminalità organizzata e simili, si traduce in una «richiesta» preventiva ed in una informazione successiva al «pubblico ministero da effettuare

---

e del Corpo della Guardia di Finanza. Cfr. L. RUSSO, *Le operazioni sotto copertura e le attività di contrasto in materia di delitti sessuali o per la tutela dei minori*, in *Giur. mer.*, 12, 2008, p. 3346.

[600] Cfr. P. FRANCESCO, *Sui rapporti tra indagini mediante agente provocatore, indagini ordinarie e sequestro probatorio del computer*, in *Dir. pen. proc.*, 2010, 10, p. 1166. D. DELL'ORTO, *Pedopornografia on line e indagini informatiche. Complessità e peculiarità tecnico-giuridiche della materia*, in *Cass. pen.*, 2007, 3042; C. MARINELLI, *L'attività dell'agente provocatore per il contrasto alla pedopornografia: "straripamenti" investigativi e relative implicazioni processuali*, in *Cass. pen.*, 2005, 2683; P. PITTARO - G. SPANGHER, *Le norme contro la pedofilia*, in *Dir. pen. proc.*, 1998, 1222; N. VENTURA, *Le investigazioni under cover della polizia giudiziaria*, Bari, 2008.

[601] Cfr., per una vivace critica all'operato degli investigatori nell'operazione "Kids Shield", D. DELL'ORTO, *Pedopornografia on line e indagini informatiche. Complessità e peculiarità tecnico-giuridiche della materia*, cit., p. 3042, nonché P. PERRI, *Profili informatico-giuridici della diffusione, mediante strumenti telematici, di materiale pedopornografico*, in *Cass. pen.*, 9, 2008, p. 3466.

al più presto e comunque entro le quarantotto ore dall'inizio delle attività». Il fine deve essere esclusivamente quello di acquisire elementi di prova in ordine ai delitti specificatamente indicati dalle leggi che giustificano tali "poteri speciali"[602]. Dal punto di vista oggettivo, infine, l'attività di indagine digitale *under cover* può estrinsecarsi in due modi: nella creazione di un *server* che consenta l'accesso a materiale pedopornografico da parte di un pubblico indeterminato, al fine di tracciare ed identificare gli eventuali fruitori (si tratta di veri e propri "siti civetta"); nella partecipazione, nonché nella realizzazione e gestione di aree di comunicazione o di scambio di materiale pedopornografico su reti o sistemi telematici. In quest'ultimo caso, l'attività di indagine consiste nell'ingresso, da parte di agenti sotto copertura, in vere e proprie *chat online*, tramite *nick name* di fantasia, al fine di prendere parte a conversazioni già in corso tra altri utenti aventi ad oggetto lo scambio di materiale pedopornografico o allo scopo di avviare comunicazioni con un pubblico indistinto, manifestando la volontà di acquisire o cedere materiale pedopornografico. Con la seguente precisazione: le condotte *under cover* devono opporsi ad iter criminosi già in corso di svolgimento, «presupponendo nel soggetto provocato un 'possesso' di beni o una serie di 'accordi finalizzati' che di per sé, secondo la normativa di riferimento, già costituiscono reato»[603]. A tal proposito va ricordato che non sono ammesse operazioni sotto copertura che si concretizzino in un incitamento o in una induzione al crimine: l'agente infiltrato non può commettere azioni illecite diverse da quelle dichiarate non punibili o ad esse strettamente e strumentalmente connesse.

Tecnologicamente affine, ma strutturalmente e funzionalmente diversa da quella appena descritta, è l'attività investigativa finalizzata alla individuazione ed all'eventuale oscuramento di quei siti *web* «utilizzati per le attività e le condotte di cui agli articoli 270-*bis* (Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico) e 270-

---

[602] «La possibilità di raccogliere fonti di prova attraverso l'attività di agenti provocatori […] ha natura del tutto eccezionale e non è suscettibile di interpretazione analogica o estensiva. Ne consegue [ad esempio] che le prove raccolte attraverso la costituzione di un sito pornografico "civetta" non sono utilizzabili nel procedimento nel quale venga contestato il delitto di cui all'art. 600 *quater* c.p., poiché quella modalità speciale di acquisizione della prova è consentita solo nelle indagini per i delitti di cui agli art. 600 *bis*, 600 ter e 600 *quinquies* c.p.». Così, Cass. pen, sez. III, 5 maggio 2004, n. 37074, in CED 230027, con nota di A. IASILLO, *Agenti provocatori e sequestro probatorio. Male captum, (non) bene retentum?*, in *Dir. e giust*., 40, 2004, p. 40. In senso conforme: Cass. pen., sez. III, 17 gennaio 2008, n. 8380, in CED 239407; Cass. pen., sez. III, 28 gennaio 2005, n. 13500, in CED 231605; Cass. pen., sez. III, 29 aprile 2004, n. 24000, in CED 228693.

[603] Si tratta della discussa distinzione tra "agente provocatore" (che non ha mai trovato definizione esplicita nella legge) e "agente infiltrato" (legislativamente prevista). Cfr. F. CAJANI, *Le operazioni digitali sotto copertura: l'agente provocatore e l'attività di contrasto nelle indagini informatiche*, cit., pp. 411 e ss.

sexies (Condotte con finalità di terrorismo) del codice penale»[604]. L'affinità si deve al contesto operativo in cui gli investigatori operano, e cioè la rete Internet, notoriamente incline ad essere utilizzata anche per scopi illeciti, soprattutto quando si parla di terrorismo. Le differenze, invece, attengono alla funzione ed al profilo oggettivo: il monitoraggio dei siti è finalizzato prioritariamente all'istituzione ed al costante aggiornamento di una *black list* dei siti Internet utilizzati per le attività connesse al terrorismo, comprese quelle di "proselitismo", di arruolamento dei *foreign fighters*, nonché di addestramento ad attività finalizzate al terrorismo, anche internazionale; tale elenco di siti è gestito dall'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (la polizia postale) e viene implementato anche attraverso le segnalazioni provenienti dagli organi di polizia giudiziaria richiamati dal comma 2 dell'articolo 7-*bis* del decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005[605]. L'autorità giudiziaria può imporre ai fornitori di connettività l'obbligo di inibire l'accesso a tali siti attraverso la creazione di appositi "filtri"[606]. Infine, il Pubblico Ministero, quando procede per i delitti di cui agli artt. 270-*bis*, 270-*ter*, 270-*quater* e 270-*quinquies* c.p. commessi con finalità di terrorismo e vi sono concreti elementi per ritenere che detti reati sono compiuti per via telematica, può con decreto motivato ordinare ai fornitori dei servizi di *hosting* o di altri servizi connessi alla rete Internet di rimuovere i singoli contenuti riguardanti i predetti delitti[607].

---

[604] Art. 2, comma 2, D.L. 18 febbraio 2015, n. 7, così modificato dalla legge di conversione 17 aprile 2015, n. 43: «Ai fini dello svolgimento delle attività di cui all'articolo 9, commi 1, lettera b), e 2, della legge 16 marzo 2006, n. 146, svolte dagli ufficiali di polizia giudiziaria ivi indicati, nonché delle attività di prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo, di cui all'articolo 7-*bis*, comma 2, del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, fatte salve le iniziative e le determinazioni dell'autorità giudiziaria, aggiorna costantemente un elenco di siti utilizzati per le attività e le condotte di cui agli articoli 270-*bis* e 270-sexies del codice penale, nel quale confluiscono le segnalazioni effettuate dagli organi di polizia giudiziaria richiamati dal medesimo comma 2 dell'articolo 7-*bis* del decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005. Il Ministro dell'interno riferisce sui provvedimenti adottati ai sensi del presente comma e dei commi 3 e 4 del presente articolo in un'apposita sezione della relazione annuale di cui all'articolo 113 della legge 1° aprile 1981, n. 121». La nuova normativa non è inedita, nel senso che già la direttiva europea sulla pedopornografia (Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile), prevedeva, all'art. 25, la possibilità di oscurare determinati siti o diminuire l'accesso a determinati dati.

[605] «… fatte salve [ovviamente] le iniziative e le determinazioni dell'autorità giudiziaria». *Ibidem*.

[606] «…secondo le modalità, i tempi e le soluzioni tecniche individuate e definite con il decreto previsto dall'articolo 14-*quater*, comma 1, della legge 3 agosto 1998, n. 269», *ex* art. 2, comma 2, D.L. 18 febbraio 2015, n. 7.

[607] *Ex* art. 2, comma 3, D.L. 18 febbraio 2015, n. 7, l'ordine deve essere adempiuto immediatamente e comunque nell'arco di quarantotto ore. In caso di inosservanza l'Autorità Giudiziaria può disporre l'interdizione all'accesso

Fuori dalla mera ricognizione normativa, un'osservazione non appare fuori luogo. Le attività *under cover* e di monitoraggio della rete da parte degli investigatori sono di estrema utilità sia in una prospettiva repressiva, sia in un contesto di prevenzione di delitti di particolare gravità, a patto che alle norme seguano gli investimenti. Fare un elenco di siti da inserire in una lista nera, anche se forse non sembra, è un adempimento tutt'altro che agevole: si tratta di un'attività che deve essere svolta nel *deepweb*[608], nella *darknet*[609], e non nel *public web*. Ed allora, o si investono risorse per la formazione degli operatori, o queste norme sono prive di senso, perché rimarranno inattuate sul piano pratico.

2. *Cloud computing*

Il *cloud computing* (in italiano, nuvola informatica) è un sistema che consente l'erogazione di servizi informatici, come l'archiviazione, l'elaborazione o la trasmissione di dati, *on demand*, attraverso la rete Internet, a partire da un insieme di risorse preesistenti e configurabili[610]. Più in dettaglio, quando si parla di *cloud* si fa riferimento ad un insieme di risorse informatiche messe a disposizione dal fornitore del servizio ad una comunità di utenti, i quali, a pagamento, condividono tali risorse, sfruttandone le potenzialità. Tali risorse non vengono completamente configurate e messe in opera dal fornitore per uno specifico utente: esse vengono assegnate, rapidamente e convenientemente, grazie a procedure automatizzate

---

di tutto il dominio internet *ex* art. 321 c.p.p. con evidente maggior danno per i soggetti che hanno disatteso l'ordine di rimuovere i singoli contenuti.

608 Il *Web* sommerso (o *deep web*), spesso erroneamente confuso con il *Dark Web* (che è invece riferito alla navigazione web in anonimato), è l'insieme delle risorse informative del *World Wide Web* non segnalate dai normali motori di ricerca. Secondo una ricerca sulle dimensioni della rete condotta nel 2000 da Bright Planet, un'organizzazione degli Stati Uniti d'America, il *Web* è costituito da oltre 550 miliardi di documenti mentre Google ne indicizza solo 2 miliardi, ossia meno del 2 per cento. Per accedere al *Web* sommerso, un utente deve utilizzare *link* diretti o specifici motori di ricerca che raccolgono i siti esclusi dai motori di ricerca comuni e *server* DNS meno selettivi sui contenuti rispetto a quelli forniti da Google o dai provider di rete internet. Data la natura controversa di molti dei siti del *deep web*, tipicamente i navigatori cercano di occultare la propria identità con programmi tipo *Tor (The Onion Router) I2P e Freenet*. Per un approfondimento, cfr. G. BRUTTO, *Deep Web: osservazioni pedo support community*, in G. COSTABILE – A. ATTANASIO – M. IANULARDO (a cura di), *IISFA Memberbook 2014. Digital forensics. Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER*, Forlì, 2015, pp. 185 e ss.

609 Una *darknet* (in italiano: rete scura) è una rete virtuale privata nella quale gli utenti si connettono solamente con persone di cui si fidano. Nel suo significato più generale, una *darknet* può essere qualsiasi tipo di gruppo chiuso e privato di persone che comunicano, ma il nome è spesso usato per reti di condivisione di file (p2p). Il termine fu coniato negli anni settanta per designare reti isolate da ARPANET (la vecchia internet) per motivi di sicurezza.

610 P. MELL, T. GRANCE, *The NIST Definition of Cloud Computing*, NIST, Special Publication 800-145, Settembre 2011.

di condivisione, lasciando all'utente parte dell'onere della configurazione. Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel *pool* condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.

La complessità tecnica del discorso appena fatto è solo apparente. Le parole chiave, quando si parla di *cloud,* sono tre: utilizzo condiviso delle risorse.

Le risorse consistono in unità di elaborazione (CPU), memorie di massa fisse o mobili, software e applicazioni dalle più svariate potenzialità, attraverso i quali un computer è in grado di elaborare, archiviare, recuperare programmi e dati.

Nel caso di computer collegati in rete locale (LAN) o geografica (WAN) la possibilità di elaborazione/archiviazione/recupero può essere estesa ad altri computer e dispositivi remoti dislocati sulla stessa rete. Sfruttando la tecnologia del *cloud computing* gli utenti collegati ad un *cloud provider* possono svolgere tutte queste mansioni anche tramite un semplice Internet *browser*. Possono, ad esempio, utilizzare software remoti non direttamente installati sul proprio computer e salvare dati su memorie di massa on-line predisposte dal provider stesso (sfruttando sia reti via cavo che senza fili). La condivisione tramite *cloud* consente l'utilizzo di strumenti tecnici altrimenti "difficilmente abbordabili" dall'utente medio.

Quanto al potenziale utilizzo, si possono distinguere tre tipologie fondamentali di servizi *cloud computing*[611]: il SaaS (*Software as a Service*), che consente l'utilizzo di programmi installati su un server remoto, cioè fuori dall'ambito proprio del computer fisico o dei computer collegati alla LAN locale; il DaaS (*Data as a Service*), attraverso il quale vengono messi a disposizione via web solamente i dati ai quali gli utenti possono accedere tramite qualsiasi applicazione come se fossero memorizzati su un disco locale; l'HaaS (*Hardware as a Service*), mediante il quale l'utente invia dati che vengono elaborati da computer remoti messi a disposizione e restituiti all'utente iniziale.

A questi tre principali servizi, possono essere aggiunti: il PaaS (*Platform as a Service*), attraverso il quale, in luogo di uno o più programmi singoli, viene eseguita in remoto una piattaforma software che può essere costituita da diversi servizi, programmi, librerie, ecc.; l'IaaS (*Infrastructure as a Service*), che consiste nella possibilità di utilizzo di risorse hardware o virtuali da remoto.

---

[611] F. MAGOULÈS, *Fundamentals of Grid Computing: Theory, Algorithms and Technologies*, U.S.A., 2010.

Già dopo questa breve premessa appaiono evidenti i vantaggi connessi all'utilizzo di servizi *cloud*: l'utente fruitore, oltre al banale utilizzo della nuvola a scopo di salvataggio remoto di dati e informazioni, potrà sfruttare le enormi potenzialità di hardware e software remoti senza averne né la titolarità, né la disponibilità fisica, il tutto grazie ad una semplice connessione a banda larga. Ovviamente, esistono anche degli svantaggi: lavorando in remoto c'è sempre il rischio di dover subire una interruzione del servizio di *clouding*, per esempio a causa di una temporanea mancanza di linea; inoltre, sui dati archiviati nei *clouds* si pone sempre un problema di riservatezza.

Parallelamente alla esponenziale crescita di servizi come *dropbox*, *google drive* ed alla capillare diffusione di *social network* come *Facebook*, in grado di creare interi ambiti virtuali in cui condividere informazioni, idee, servizi, interessi e comunicazioni, è cresciuta l'importanza di svolgere indagini di polizia giudiziaria su sistemi *cloud*.

Dal punto di vista tecnico, si tratta di attività ad alto contenuto tecnologico, normalmente affidate a tecnici altamente specializzati: il *cloud* non può essere "spento" o "sospeso", quindi è necessario intervenire sui dati in modo dinamico, captandoli nel loro fluire[612].

Dal punto di vista giuridico, al di là delle problematiche di diritto penale internazionale connesse alla mancanza di territorialità e di identificabilità tipica delle "nuvole"[613], le informazioni "esternalizzate" sono accessibili coattivamente da parte dell'autorità giudiziaria inquirente, sia tramite decreto di ispezione, *ex* art. 244, co. 2, c.p.p., sia tramite decreto di perquisizione, a norma dell'art. 247, co. 1-*bis*, c.p.p. Quanto all'apprensione ed al repertamento dei dati contenuti nella "nuvola", l'autorità giudiziaria può senz'altro chiedere ai gestori (fornitori di servizi informatici, telematici o di telecomunicazioni) che l'acquisizione di tali dati avvenga «mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità», così come prevede l'art. 254-*bis* del codice di rito.

Nulla quaestio circa la legittimità di tali iniziative tipiche e palesi dell'autorità, a fronte delle quali peraltro il bacino di garanzie difensive è piuttosto ampio e comprende la

---

[612] Per un approfondimento, cfr. S. ATERNO – M. MATTIUCCI, *Cloud forensics e nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. pen.*, 2013, 3, p. 865.

[613] Tutti i servizi descritti implicano la memorizzazione dei dati dell'utente in *server farms* che potrebbero essere localizzate, per i motivi più disparati, in un Paese diverso sia da quello di appartenenza del fornitore del servizio, sia di quello dell'utente finale. Qualora sia necessario, per esigenze di indagine, l'acquisizione forzata di tali dati, ciò comporta un evidente problema di diritto penale internazionale. Il giudice competente ad adottare eventuali provvedimenti autoritativi sui dati archiviati nei *clouds* dipende dal tipo di criterio adottato per determinare la giurisdizione. Per una disamina completa di tale problema, cfr. G. M. RUOTOLO, *Hey! You! Get off my cloud!*, in *Archivio Penale*, settembre-dicembre 2013, fasc. 3, pp. 857 e ss.

conoscibilità dell'atto (art. 250 c.p.p.), l'assistenza del difensore (art. 365) ed il deposito del verbale (art. 366), con facoltà di accesso a tale atto da parte della difesa.

Più problematica appare, invece, l'ammissibilità di un accesso occulto alla nuvola, attraverso, ad esempio, un *virus* di Stato. Con riferimento a tale tipologia di attività si ripresentano ancora una volta tutti i problemi già analizzati in relazione alla legittimità di tale prova atipica alla luce dell'attuale quadro costituzionale.

3. Il controllo occulto mediante OSint: natura e limiti di ammissibilità

Secondo una definizione ampiamente accettata in dottrina, con il termine OSint[614] si intende indicare l'informazione -disponibile ed aperta all'accesso pubblico- che ha subito un filtro di ricerca, selezione, distillazione e diffusione al fine di soddisfare un preciso bisogno informativo, espresso da un *Intelligence Requirement*[615].

La c.d. "analisi delle fonti aperte" fa parte integrante dell'attività di *intelligence*[616] e si avvale di diversi strumenti: mezzi di comunicazione di massa (giornali, riviste, televisione, radio e siti web); dati pubblici (rapporti dei governi, piani finanziari, dati demografici, dibattiti legislativi, conferenze stampa, discorsi, avvisi aeronautici e marittimi); file multimediali (video, audio, fotografie e mappe); informazioni provenienti da database istituzionali o privati, anche a pagamento. Internet, in particolare, offre diverse fonti da cui acquisire informazioni (siti web, blog, social network, forum, canali IRC, reti P2P, TOR, ecc.). Ovviamente, una efficace attività investigativa Osint basata sulla rete non può fare a meno dell'ausilio di adeguati strumenti software[617], a prescindere dal ruolo e dalla competenza dell'analista.

---

[614] OSint (Open Source Intelligence), ovvero raccolta, valutazione ed analisi di dati provenienti da fonti eterogenee di dominio pubblico.

[615] Così, F. MINNITI, *Ricerca CeMISS C8/Z. Le fonti informative e l'open source*, su www.difesa.it/SMD_/CASD/IM/CeMISS/Pubblicazioni/Documents/42175_Minniti_0pdf.pdf.

[616] Che, secondo uno schema classico, consta di almeno cinque fondamentali attività: *Humint* (*human intelligence*); *Sigint* (*signals intelligence*); *Imint* (*imagery intelligence*); *Osint* (*open source intelligence*); *Masint* (*measurement and signature intelligence)*. Per un approfondimento, cfr. L. REITANO, *Esplorare Internet. Manuale di investigazioni digitali e Open Source Intelligence*, Bologna, 2014, pp. 19 ss.

[617] Quali, ad esempio: "FOCA" (utile per estrarre informazioni dai file contenuti in un de- terminato sito web); "Maltego" (usato per individuare ed organizzare relazioni tra persone e gruppi di persone, imprese e organizzazioni presenti sul web); "Webzip" (indispensabile per "scaricare" ed archiviare su di un proprio supporto l'intero contenuto -link compresi– di un sito web); "Copernic pro" (trattasi di un metamotore di ricerca in grado di ricercare un set di parole chiave su più motori di ricerca contemporaneamente); "Cmap" (indispensabile per la rappresentazione grafica esplicativa delle relazioni intercorrenti tra le diverse entità

I dati estrapolati, se opportunamente analizzati, cioè correlati e validati in termini di attendibilità e pertinenza, rappresentano un utile supporto informativo nelle indagini riguardanti sia reati informatici, sia reati di tipo tradizionale[618].

L'Open Source Intelligence (o OSint) dovrebbe utilizzare esclusivamente fonti aperte ed ottenere, dunque, informazioni "non classificate", e cioè informazioni disponibili al pubblico, anche se non necessariamente ad alta divulgazione o ad accesso gratuito.

Il problema, tuttavia, è che tale specifica azione informativa, caratterizzata da tempestività, aderenza e continuità, rischia di entrare in conflitto con la tutela di fondamentali diritti della persona, dalla "riservatezza" sino alla cd. "autodeterminazione informativa"[619].

La soluzione circa la legittimità o meno dell'attività di indagine in argomento dipende dal tipo di informazione estrapolata in modo occulto e, in particolare, dall'aspettativa di riservatezza che il soggetto ripone su di essa[620].

Partendo da questo peculiare angolo di osservazione, privilegiato dal giurista, è possibile distinguere i dati pubblici, o di pubblico dominio, dai dati riservati. Nell'ambito dei social network, dati pubblici possono essere definiti tutti quei contenuti digitali immessi volontariamente dall'utente sul proprio profilo personale e destinati ad una comunità indistinta di fruitori. Il social network *Facebook*, ad esempio, consente agli iscritti di creare una propria pagina nella quale è possibile pubblicare immagini, filmati ed altri contenuti multimediali. Ovviamente, l'accesso a questi contenuti è regolato attraverso impostazioni sulla privacy prestabilite dall'utente. Tuttavia, le informazioni e le fotografie pubblicate sul profilo e non assistite da particolari filtri di visibilità non sono possono considerarsi riservate e non godono, quindi, di tutela sotto il profilo della loro eventuale divulgazione ad opera di terzi fruitori. In

---

presenti sul web); "Google Hacks" (che consente di creare query complesse in grado di individuare eventuali aspetti di vulnerabilità di un sito web); "Didtheyreadit" (programma in grado di tracciare la posta elettronica inviata, restituendo al mittente informazioni sul destinatario, tipo geolocalizzazione, sistema operativo utilizzato, ecc.); "VisualRoute" (software ideato per individuare il percorso seguito dai nostri dati su Internet); ecc.

[618] «Basti pensare che circa l'80% delle informazioni utili per una investigazione al momento provengono dalle "fonti aperte"». Così, G. ZAPPULLA, *Consultant and Strategist on Risk Management and Intelligence*, in L. REITANO, *Esplorare Internet. Manuale di investigazioni digitali e Open Source Intelligence*, cit., p. 8.

[619] «Il "diritto all'autodeterminazione informativa" va oltre la tutela della privacy. Esso conferisce alla persona, in linea di principio, il potere di determinare, in sé, la divulgazione e l'utilizzo dei suoi dati personali [ampliando] la tutela della libertà della vita privata in termini di diritti fondamentali»: così, BVerfG 370/2007-595/2007, 27.02.2008, in CR, 2008, tradotta in italiano e consultabile grazie al contributo di R. FLOR, *La sentenza del Bundesverfassungsgericht del 27 febbraio 2008 sulla c.d. online durchsuchung*, cit., p. 682. Si veda, altresì, M.P. ADDIS, *Diritto all'autodeterminazione informativa e processo penale in Germania*, in D. NEGRI (a cura di), *Protezione dei dati personali e accertamento penale*, Roma, 2007, p. 91.

[620] In altre parole, è indispensabile classificare i dati digitali presenti in un social network in funzione della loro accessibilità. Così, G. VACIAGO, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, 2012, p. 120.

altri termini, nel momento in cui si pubblicano informazioni e foto sulla pagina dedicata al proprio profilo personale, rendendole accessibili *erga omnes*, si accetta il rischio che le stesse possano essere portate a conoscenza anche di terzi non rientranti nell'ambito delle c.d. amicizie accettate dall'utente.

Riservate, invece, sono quelle informazioni che l'utente ritiene di voler condividere esclusivamente con la sua cerchia di "amici". Si tratta di informazioni accessibili esclusivamente da persone selezionate dall'utente come potenziali fruitori dei dati contenuti nel proprio profilo social network, con conseguente esclusione di tutti coloro che, iscritti o non iscritti, non sono stati autorizzati. Si tratta di informazioni che l'utente nasconde attraverso idonee misure e che decide di condividere esclusivamente con se stesso o, al più, con una o più persone ben specificate (all'uopo autorizzate all'accesso a tali informazioni)[621].

Ebbene, non presenta particolari problemi interpretativi la facoltà della polizia giudiziaria di avvalersi autonomamente nel corso delle indagini di tutti i dati pubblicamente accessibili in rete[622]. Si tratta di una sorta di "pedinamento virtuale" che rientra in quell'attività atipica[623] *ex* artt. 55 e 348 del codice di rito, senza necessità di un previo provvedimento autorizzativo della magistratura[624].

Quanto ai dati riservati, la loro acquisizione ed il loro sfruttamento per fini investigativi non rientra nell'ambito dell'OSint, che, per definizione, si avvale di fonti aperte. Quindi, ufficialmente, la polizia giudiziaria può ottenere questo tipo di informazioni esclusivamente

---

[621] Quanto a *Facebook*, ad esempio, dal 31 maggio 2010 è possibile applicare le impostazioni di privacy anche ai singoli post o ai singoli commenti. Inoltre è stata estesa la lista dei "livelli", aggiungendo anche un livello personalizzato. I livelli disponibili sono: "Solo Io", "Amici", "Amici di amici", "Amici e reti", "Tutti", "Personalizzato". Questi livelli possono essere impostati indipendentemente per ciascuna "categoria" di informazioni del profilo, sui singoli dati (commenti, post, ecc.) oppure sui dati personali (come "Data di nascita", "Orientamento politico e religioso", "Istruzione e lavoro", ecc.). Agendo opportunamente sulle impostazioni del profilo è quindi possibile limitare la diffusione dei dati personali. In particolare, nel menù "Impostazioni" è disponibile la voce "Impostazioni sulla privacy", dalla quale sarà possibile agire sulle categorie di dati tra cui: profilo, ricerca, notizie e bacheca. Cfr. http://it.wikipedia.org/wiki/Facebook.

[622] Detto con uno slogan che rende l'idea, «se riveli al vento i tuoi segreti, non devi poi rimproverare al vento di rivelarli agli alberi» (KAHLIL GIBRAN, scrittore, poeta e filosofo libanese – 6 gennaio 1883, 10 aprile 1931).

[623] Come noto, la giurisprudenza considera il pedinamento (tradizionale) atto atipico di polizia giudiziaria non intrusivo della sfera privata, in quanto non intacca la libertà morale dell'individuo (controllato a sua insaputa ed in luoghi pubblici o aperti al pubblico). Così, Cass., sez. II, 30 ottobre 2008, n. 44912, in *CED Cass.*, n. 230027.

[624] «Il diritto alla riservatezza [...] non viene intaccato se la misura – di monitoraggio segreto di Internet [...] – è limitata ai dati che il titolare del sistema ha fornito tramite una comunicazione in Internet, in quanto tale soggetto ha "aperto" il suo sistema, in termini tecnici. Pertanto, non può fare affidamento su tale situazione, che può comportare la raccolta dei dati (omissis). In tali ipotesi, ed in linea di principio, allo Stato non è negata la possibilità di ottenere informazioni accessibili al pubblico». Così, BVerfG 370/2007-595/2007, 27.02.2008, in CR, 2008, cit.

attraverso la collaborazione del gestore del social[625]. Naturalmente, il riferimento è ai dati di carattere non comunicativo, giacché per i contenuti comunicativi occorre rispettare la disciplina delle intercettazioni[626].

Circoscrivendo l'analisi al più noto e diffuso social in circolazione (*Facebook*), si osserva che le forze dell'ordine possono formulare richiesta di dati riservati attraverso le seguenti fondamentali modalità: telematicamente (attraverso l'accesso al *Request Secure Access to the Law Enforcement Online Request System*[627]) oppure tramite email[628], fax[629] o posta ordinaria[630].

---

[625] Cfr. le "informazioni per le forze dell'ordine" presenti sul sito https://it-it.facebook.com/safety/groups/law/guidelines. Un caso a parte è rappresentato da quei dati e da quelle informazioni il cui consenso alla condivisione viene carpito con l' "inganno". Ci si riferisce, in particolare, all'ipotesi della polizia giudiziaria che si finge "amica" su Facebook della persona sottoposta alle indagini, al fine di farsi "accettare" e diventare, di conseguenza, fruitore di tutte quelle informazioni che, altrimenti, le sarebbero precluse dal filtro di riservatezza (solo amici) impostato dall'utente. Una siffatta attività investigativa è da ritenersi legittima nei limiti in cui è finalizzata ad "accedere passivamente" ai dati che la persona ha inteso riservare ai soli amici. Si pensi, ancora, alla polizia giudiziaria che si metta d'accordo con un amico ed acceda alle informazioni mediante l'aiuto di tale soggetto. Maggiori problemi sorgono qualora l'attività si estrinsechi in una vera e propria "provocazione telematica": non essendo prevista –con riferimento alla generalità dei reati e salvo le ipotesi di indagini finalizzate al contrasto della pedopornografia *online* e reati assimilati– la c.d. "attività sotto copertura on line", tale azione investigativa parrebbe da ritenersi illegittima.

[626] In questo senso si è espressa di recente la giurisprudenza di merito, secondo la quale «il social network Facebook si caratterizza, tra l'altro, per il fatto che ciascuno degli iscritti, nel registrarsi, crea una propria pagina nella quale può inserire una serie di informazioni di carattere personale e professionale e può pubblicare, tra l'altro, immagini, filmati ed altri contenuti multimediali; sebbene l'accesso a questi contenuti sia limitato secondo le impostazioni della privacy scelte dal singolo utente, deve ritenersi che le informazioni e le fotografie che vengono pubblicate sul proprio profilo non siano assistite dalla segretezza che, al contrario, accompagna quelle contenute nei messaggi scambiati utilizzando il servizio di messaggistica (o di chat) fornito dal social network; mentre queste ultime, infatti, possono essere assimilate a forme di corrispondenza privata, e come tali devono ricevere la massima tutela sotto il profilo della loro divulgazione, quelle pubblicate sul proprio profilo personale, proprio in quanto già di per sé destinate ad essere conosciute da soggetti terzi, sebbene rientranti nell'ambito della cerchia delle c.d. "amicizie" del social network, non possono ritenersi assistite da tale protezione, dovendo, al contrario, essere considerate alla stregua di informazioni conoscibili da terzi. In altri termini, nel momento in cui si pubblicano informazioni e foto sulla pagina dedicata al proprio profilo personale, si accetta il rischio che le stesse possano essere portate a conoscenza anche di terze persone non rientranti nell'ambito delle c.d. "amicizie" accettate dall'utente, il che le rende, per il solo fatto della loro pubblicazione, conoscibili da terzi ed utilizzabili anche in sede giudiziaria». Così, Trib. Santa Maria Capua Vetere, Ufficio Volontaria Giurisdizione, Decreto del 13 giugno 2013, consultabile al seguente URL: http://www.altalex.com/index.php?idnot=63789. Il caso riguardava una separazione consensuale, oggetto di successivo ricorso da parte di uno dei coniugi (la moglie) per l'intervenuta modifica delle sue condizioni economiche. Ebbene, il marito respingeva la pretesa, da parte della moglie, di un assegno di mantenimento provando la sua stabile relazione con un terzo soggetto proprio attraverso alcune immagini della donna in compagnia del nuovo compagno convivente, prelevate dal profilo Facebook della moglie.

[627] Dedicato agli operatori di polizia giudiziaria e disponibile al seguente link: https://www.facebook.com/records/x/login.

[628] Al seguente indirizzo: records@fb.com.

[629] Stati Uniti: +1 650 472-8007; Irlanda: +353 (0)1 653 5373.

[630] Indirizzo negli Stati Uniti: 1601 Willow Road, Menlo Park CA 94025; indirizzo in Irlanda: Hanover Reach | 5-7 Hanover Quay, | Dublin 2.

Il *Facebook Security, Law Enforcement Response Team* evade le richieste pervenute sulla base di precisi criteri, «nel rispetto delle […] condizioni di servizio e delle leggi applicabili, compreso il *Federal Stored Communications Act* ("SCA"), 18 U.S.C. Sezioni 2701-2712»[631].

In base alla legge statunitense, che in questo procedimento viene in rilievo, «Per procedere alla divulgazione di dati di base di un abbonato, è necessario un decreto ingiuntivo valido, rilasciato in connessione con un'investigazione di natura penale (18 U.S.C. Sezione 2703(c)[…]. Per obbligare Facebook a rivelare informazioni specifiche o altri dati relativi agli account, tra cui intestazioni di messaggi e indirizzi IP[632], in aggiunta ai dati essenziali sugli utenti di cui sopra[633], è necessaria un'ingiunzione del tribunale, come previsto dal Titolo 18 U.S.C., Articolo 2703(d). Sono invece esclusi i contenuti delle comunicazioni. Per obbligare Facebook a rivelare i contenuti memorizzati su un qualsiasi account, tra cui messaggi, foto, video, post in bacheca e informazioni sui luoghi, è necessario che, alla luce di "fondati motivi", venga emesso un mandato di perquisizione in conformità alle procedure contenute nelle *Federal Rules of Criminal Procedure* o ad altre procedure statali sui mandati di perquisizione equivalenti»[634]. Con una precisazione: «potrebbe essere necessaria una richiesta *Mutual Legal Assistance Treaty* o una rogatoria per ottenere il rilascio dei contenuti di un account»[635].

---

631 «Negli USA, le intercettazioni telematiche [sono] regolate dall'*Electronic Privacy Communications Act* emanato nel 1986. Con l'emanazione di questo atto, è stato chiarito che ogni intercettazione che non rispetti le condizioni previste dalla legge, deve essere considerata illegale e, oltre a comportare l'inutilizzabilità di tali informazioni all'interno del processo, può determinare un'azione di risarcimento del danno rivolta nei confronti del responsabile. Questa normativa è divisa in tre titoli: il primo è dedicato specificamente alle intercettazioni delle comunicazioni telematiche (Electronic Privacy Communications Act, 18 U.S.C. § 2510), il secondo regola la possibilità di accedere ai contenuti memorizzati all'interno di un computer o di un server (Stored Communications Act, 18 U.S.C. § 2701) e il terzo riguarda la possibilità di monitorare gli accessi alla Rete da parte degli utenti, senza tuttavia poter conoscere il contenuto delle loro comunicazioni (Pen Register Act, 18 U.S.C. § 206). [...]». G. VACIAGO, *Privacy e tutela dell'ordine pubblico in Europa e negli Stati Uniti: un differente approccio per raggiungere un difficile compromesso*, in *Informatica e diritto*, vol. XVIII, 2009, n. 1, p. 135 ss.

632 «L'indirizzo IP è un numero che identifica un dispositivo collegato a una rete telematica: esso può essere paragonato ad un indirizzo stradale o ad un numero telefonico. Il fornitore di connettività, infatti, dato un indirizzo IP e l'ora di accesso a tale indirizzo, è in grado di fornire i dati personali di chi ha sottoscritto il contratto per usufruire dei servizi di connessione. L'indirizzo IP, in sé, non offre nessuna informazione utile all'indagine, ma senza di esso non sarebbe possibile ottenere le corrette informazioni da parte del fornitore di connettività». G. VACIAGO, *Privacy e tutela dell'ordine pubblico in Europa e negli Stati Uniti*, cit., p. 139.

633 Ibidem: «I dati digitali che vengono generalmente richiesti in ambito investigativo possono generalmente dividersi fra quelli che consentono l'identificazione di un potenziale criminale (indirizzo IP), quelli che ne determinano l'attività on line (log files) e quelli che consentono di conoscere le sue conversazioni (intercettazioni telematiche)».

634 Cfr. le "informazioni per le forze dell'ordine" presenti sul sito https://it-it.facebook.com/safety/groups/law/guidelines.

635 *Ibidem*.

In Italia, codice della privacy[636] alla mano, tali richieste di informazioni da parte delle forze dell'ordine possono considerarsi legittime nei limiti di seguito descritti.

Bisogna distinguere tra richieste di informazioni formulate nell'ambito di attività di indagine di polizia giudiziaria e richieste avanzate da pubbliche autorità per altre finalità istituzionali.

Le prime rientrano nei "trattamenti di dati personali" effettuati per «ragioni di giustizia» (art. 8, comma 2, lett. g, codice della privacy)[637] ovvero «per finalità di prevenzione, accertamento o repressione di reati» (art. 53, comma 1, codice della privacy)[638]. In entrambi i casi deve darsi corso a tali richieste purché sia chiaro il riferimento ad una attività di polizia giudiziaria, non ostandovi l'applicabilità del codice sulla privacy. Ed infatti, a norma dell'art. 132 del Codice in materia di protezione dei dati personali, «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»[639]. Tuttavia, in ossequio al principio di pertinenza, per quanto possibile le informazioni divulgate dovranno essere circostanziate sotto il profilo oggettivo e temporale.

Viceversa, qualora le richieste avanzate da forze di polizia o da altre pubbliche autorità non siano riconducibili all'esercizio di poteri di polizia giudiziaria, trova applicazione la disciplina generale a tutela della privacy, in base alla quale un soggetto può permettere l'accesso a dati personali solo in adempimento di un obbligo legale, o, in alternativa, in presenza del consenso dell'interessato (cfr. artt. 23, comma 1, e 24, comma 1, lett. a, codice della privacy).

Ciò chiarito, merita precisare che nella prassi operativa queste informazioni vengono ottenute attraverso la c.d. *online surveillance*[640], ossia la tecnica (di cui abbiamo già ampiamente discusso *supra*) che consente agli investigatori di rilevare e registrare da remoto ed in tempo reale tutto ciò che accade attraverso un determinato dispositivo (personal computer, tablet, smartphone, ecc.). Nel momento in cui il soggetto attenzionato sfrutta tale dispositivo allo scopo di gestire *online* il proprio profilo registrato su un determinato social

---

[636] D. Lgs. 30 giugno 2003, n. 196 , in G.U. 29 luglio 2003 ,aggiornato al d. lgs. 14 marzo 2013, n. 33.
[637] Quando le richieste di informazioni sono effettuate su delega dell'autorità giudiziaria.
[638] Quando derivano da un'attività investigativa o d'indagine di iniziativa degli organi di polizia.
[639] Si veda C. CONTI, *Attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, in S. LORUSSO (a cura di), *Le nuove norme sulla sicurezza pubblica*, Padova, 2008, pp.14 ss.
[640] Prassi che fa volentieri a meno, per ovvie ragioni, delle lungaggini tipiche di una rogatoria internazionale.

network, tale attività viene monitorata e carpita. Si tratta di un tema che, ancora una volta, si intreccia con quello della legittimità dei c.d. *virus trojan* e delle *backdoors*[641] di Stato.

[641] Le *backdoors* in informatica sono paragonabili a porte di servizio (cioè le porte sul retro) che consentono di superare in parte o in tutto le procedure di sicurezza attivate in un sistema informatico o in un computer entrando nel sistema stesso.

CONSIDERAZIONI CONCLUSIVE

Fino ad un passato non troppo remoto la prova regina nel processo penale era la testimonianza, definibile come narrazione di un fatto accaduto, compiuta da un soggetto estraneo al processo, che di quel fatto abbia avuto conoscenza diretta o indiretta.

Oggi, invece, atteso che un numero sempre più elevato di circostanze rilevanti per il processo può essere dimostrato soltanto con elementi tecnici sofisticati, guardare al futuro del processo penale significa soprattutto parlare di prova scientifica, ossia della progressiva adozione di modelli scientifici da utilizzare nell'indagine sui fatti[642].

Tale evoluzione del processo rappresenta, come già detto, una fisiologica conseguenza del progresso tecnologico. La tecnologia, infatti, rafforza la criminalità e la sua mutevole capacità distruttiva; è pertanto inevitabile che si registri una reazione da parte dell'ordinamento. Criminalità più forte implica parallelamente indagini più penetranti e più insidiose: si tratta di una reazione inesorabile alla quale nessun sistema può sottrarsi.

Le indagini informatiche si collocano in questo contesto di contrasto e di contenimento dei rischi di lesione e di messa in pericolo di tradizionali e nuovi beni giuridici ed il processo penale non può farne a meno. Certo, tutto ciò non più che destare preoccupazione: la promiscuità dei dati, l'impossibilità tecnica di un accesso selettivo al sistema informatico, il rischio sempre presente che queste indagini si trasformino in attività esplorative, lo spazio informatico ontologicamente globale e refrattario a qualsiasi limitazione nazionale fanno delle investigazioni di natura digitale la forma di indagine più insidiosa che esista.

I nodi problematici della materia attengono sia all'aspetto soggettivo, inteso come necessaria tutela dei diritti e delle libertà fondamentali della persona coinvolta nell'accertamento processuale, sia all'aspetto oggettivo, relativo alla maggiore o minore attendibilità del metodo scientifico utilizzato per fini forensi.

Le indagini tipiche (ispezioni, perquisizioni, sequestri, rilievi urgenti e accertamenti tecnici di natura digitale) pongono non pochi problemi con riferimento, soprattutto, alla "genuinità" della prova digitale unilateralmente raccolta. L'antidoto, in questi casi, è quello di assicurare il contraddittorio nella formazione della prova, privilegiando una dialettica tecnica anticipata

[642] M. DAMASKA, *Il diritto delle prove alla deriva*, Bologna, 2003.

laddove le circostanze contingenti lo consentano senza mettere a rischio la conservazione della prova.

Come abbiamo visto, le perquisizioni *online* pongono questioni ancora maggiori: da un lato, vi è un problema di attendibilità e genuinità che si annida nell'oscuro terreno delle tecniche mediante le quali simili attività vengono attuate; dall'altro, anche qualora si dovesse raggiungere una soluzione sul fronte dell'attendibilità dell'informazione acquisita, resterebbe il difficilmente superabile problema dell'invasività. L'impiego dei virus, infatti, attua una forma di controllo che, anche a prescindere dal tipo di dato captato, si connota *ex se* per un livello inusitato di ingerenza nella vita privata. Lo spionaggio occulto, effettuato in modo continuativo ed in tempo reale, di ogni attività svolta con il proprio computer va oltre la semplice "somma" dei dati captati. Ed allora, una riflessione su questo tema non è assolutamente rinviabile e si dovrebbe procedere ad introdurre una normativa *ad hoc* all'interno dello stesso codice di procedura penale. *Medio tempore*, all'interprete è richiesto un approccio che realizzi un'integrazione del diritto con la tecnica e che si concluda con un "dominio" del primo sulla seconda.

Quanto alle altre indagini informatiche occulte (intercettazioni telematiche, pedinamento elettronico, *data retention*, operazioni digitali sotto copertura, monitoraggio dei siti, *Osint*), è necessario un approccio competente: gli atteggiamenti generalizzanti di totale rifiuto dei nuovi strumenti investigativi, così come le critiche adesioni ai postulati della scienza giustificate dalle esigenze della prassi costituiscono entrambi approcci politicamente scorretti, prima che assolutamente antigiuridici. Occorre dunque sforzarsi per mantenere alto il livello di aggiornamento e la specificità di conoscenze e di competenze della tecnologia informatica, al fine di far rivivere i principi nella dimensione specifica e concreta che oggi questi devono assumere.

Seguendo rigorosamente tale approccio, al fine di acquisire dati utili all'accertamento processuale –e nei limiti in cui, anche sotto un profilo tecnico, ciò sia possibile– è necessario limitarsi a ricorrere alle attività tipiche o atipiche consentite dall'ordinamento, in quanto in linea con i principi fondamentali del sistema, così come estrapolabili dal codice di rito e, prima ancora, dalla Costituzione. Per il resto, ci è caro ricordare un insegnamento antico ma

ancora attuale, in base al quale, «allo Stato e alla comunità internazionale [...] compete [...] il compito di disciplinare l'uso dei progressi tecnici entro rigorosi schemi giuridici»[643].

Nelle indagini digitali la tensione tra esigenze di garanzia individuali ed esigenze di difesa sociale appare in tutta la sua intensità. Un dato, tuttavia, ci preme sottolineare: la criminalità, per quanto cruenta, non potrà mai di per sé abbattere direttamente uno stato di diritto, ma potrà costringerlo all'autodistruzione nel momento in cui la democrazia, per combattere la criminalità, abdicherà rinunciando ai suoi pilastri fondamentali. Quindi, lotta della democrazia contro le organizzazioni criminali, ma soprattutto lotta della democrazia contro se stessa e contro le proprie pulsioni all'autodistruzione. Ebbene, non esiste lotta più difficile di quella in cui il nemico è rappresentato da noi stessi.

«C'è un mondo giuridico da riadattare alle tecnologie della sicurezza. E chi ritiene che nell'era delle stragi per strada sia un lusso, forse trascura che questi strumenti di controllo delle comunicazioni, e quindi dell'identità profonda delle persone, sono un po' come gli spiriti della lampada: una volta che (a motivo, ad esempio, della sicurezza antiterrorismo) siano usciti dalla lampada per entrare da padroni nei telefoni e computer delle persone, non si sa più se e quando i loro Aladino securitari saranno disposti a farceli rientrare»[644].

---

643 G. VASSALLI, *La protezione della sfera della personalità nell'era della tecnica*, in AA.VV., *Studi in onore di Emilio Betti*, vol. V, Milano, 1962, p. 684.

644 L. FERRARELLA, *Tecnologia per la sicurezza, ma tuteliamo anche la privacy*, in Corriere della Sera, 9 dicembre 2015.

BIBLIOGRAFIA

A

ABEL, W., *La decisione della corte costituzionale tedesca sul diritto alla riservatezza ed integrità dei sistemi tecnologici d'informazione - un rapporto sul caso BVerfGE*, NJW 2008, 822, disponibile su www.jei.it, 30 novembre 2015.

ADDIS, M. P., *Diritto all'autodeterminazione informativa e processo penale in Germania*, in D. NEGRI (a cura di), *Protezione dei dati personali e accertamento penale*, Roma, 2007.

ALCARO, F., *Riflessioni "vecchie" e "nuove" in tema di beni immateriali. Il diritto d'autore nell'era digitale*, in *Rass. dir. civ.*, 2006, p. 951.

ALLEGREZZA, S., *Giustizia penale e diritto all'autodeterminazione dei dati nella regione europea*, in AA.VV., *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, a cura di D. NEGRI, Roma, 2007.

ALLEGREZZA, S., *Le misure coercitive nelle «Model Rules for the Procedure of the European Public Prosecutor's Office»*, in F. RUGGIERI, T. RAFARACI, G. DI PAOLO, S. MARCOLINI, R. BELFIORE (a cura di), *Processo penale, lingua e Unione Europea*, Padova, 2013.

ALLEGREZZA, S., *Verso una Procura europea per tutelare gli interessi finanziari dell'Unione. Idee di ieri, chances di oggi, prospettive di domani*, in *Dir. Pen. Cont*., 31 ottobre 2013.

AMATO, G., *L'intercettazione ambientale non può avvenire in qualunque luogo si trovi il soggetto*, in *Il Sole 24 Ore*, 5 ottobre 2015.

AMODIO, E., *Libero convincimento e tassatività dei mezzi di prova: un approccio comparativo*, in *Riv. it. dir. proc. pen.*, 1999, p. 3.

ANGELICI, C., voce *Documentazione e documento*, in *Enc. giur. Treccani*, XI, Roma, 1989.

ANGELOSANTO, P., *Le intercettazioni telematiche e le criticità del* data retention *nel contrasto alla criminalità organizzata*, *Atti del convegno "Intercettazioni, tra esigenze investigative e diritto alla privacy"* – Palermo, 17-18 gennaio 2014, www.sicurezzaegiustizia.com, 30 novembre 2015.

APRILE E., voce *Captazioni atipiche (voci, immagini, segnali)*, in A. SCALFATI (diretto da), *Dig. proc. pen. online*, Torino, 2012.

APRILE, E., *Le indagini tecnico-scientifiche: problematiche giuridiche sulla formazione delle prova penale*, in *Cass. pen.*, 2003, p. 4036.

APRILE, E., - SPIEZIA, F., *Le intercettazioni telefoniche e ambientali*, Milano, 2004.

APRUZZESE, V., *Dal computer crime al computer-related crime*, in *Rivista di criminologia, vittimologia e sicurezza*, 2007, pp. 55 e ss.

ATERNO, S., *Acquisizione e analisi della prova informatica*, in *Dir. pen. proc*., 2008, p. 62.

ATERNO, S., *Digital forensics (investigazioni informatiche)*, in *Dig. disc. pen. (agg.)*, 2014, p. 217-247.

ATERNO, S., *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del* cloud criminal, in COSTABILE, G., - ATTANASIO, A. (a cura di), *IISFA Memberbook 2012 Digital Forensics. Condivisione della conoscenza tra i membri dell'IISFA Italian Chapter*, Forlì, 2013.

ATERNO, S., *Modifiche al titolo III del libro terzo del codice di procedura penale*, in AA.Vv., *Cybercrime, responsabilità degli enti, prova digitale. Commento alla legge 18 marzo 2008, n.48*, a cura di G. CORASANITI - G. CORRIAS LUCENTE, Padova, 2009.

ATERNO, S., – MATTIUCCI, M., *Cloud forensics e nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. pen.,* 2013, 3, p. 865.

B

BARBIERI, A., *Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici (commento a l. 18 marzo 2008, n. 48)*, in *Diritto dell'*Internet, 2008, pp. 516 e ss.

BARGIS, M., *Note in tema di prova scientifica nel processo penale*, in *Riv. dir. proc.*, 2011, pp. 47 e ss.

BASSI, V., *Alcune riflessioni in materia di atti irripetibili alla luce della novella n. 356/92*, in *Cass. pen.*, 1994, pp. 2112 e ss.

BASSO, E., *Commento agli artt. 244-246*, in *Commento al nuovo c.p.p.*, coordinato da M. CHIAVARIO, III, Torino, 1990.

BATTAGLIO, S., *"Indizio" e "prova indiziaria" nel processo penale*, in *Riv. it. dir. proc. pen.*, 1995, p. 375.

BECCARIA, C., *Dei delitti e delle pene*, Livorno, 1764.

BELLANTONI, G., *Sequestro probatorio e processo penale*, Piacenza, 2005.

BELLORA, C., *Ispezione giudiziale*, in *Dig. disc. pen.*, VII, Torino, 1993, p. 276.

BONSIGNORE, V., *L'acquisizione di copie in luogo del sequestro: un atto atipico delle garanzie difensive*, in *Cass. pen.*, 1998, p. 1504.

BONZANO, C., *Attività del pubblico ministero*, in G. GARUTI (a cura di), *Le Indagini preliminari e l'udienza preliminare* in *Trattato di procedura penale*, Vol. III, diretto da G. SPANGHER, Torino, 2009.

BONZANO, C., *Il segreto di Stato nel processo penale*, Padova, 2010.

BORRELLI, G., *Riprese filmate nel bagno di un pubblico esercizio e garanzie costituzionali*, in *Cass. pen., 2001*, p. 2446.

BOTTI, C., *Ma il sensore posto nell'autoveicolo potrebbe violare il domicilio*, in *Dir. e giust.*, 2002, 22, p. 17.

BOZIO, V., *La prova atipica*, in P. FERRUA - E. MARZADURI – G. SPANGHER (a cura di), *La prova penale*, Torino, 2013.

BRACCI, A., *Aspetti penali della disciplina delle sostanze stupefacenti e psicotrope*, in *Polizia Moderna*, suppl. al n. 5, p. 73.

BRAGHÒ, L., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in AA.VV. (a cura di L. LUPARIA), *Sistema penale e criminalità informatica*, Milano, 2009.

BRENNER, S. W., *Fourth Amendment Future: Remote Computer Searchesand the Use of Virtual Force*, in *81 Miss. L. J.*,1, 2011.

BRUNO, O., *L'esaltazione di un'impronta digitale non configura un'ipotesi di accertamento tecnico irripetibile*, in *Proc. pen. giust.*, 5, 2013, p. 54.

BRUNO, O., *Un passo avanti: il confronto delle impronte digitali postula il rigore dell'art. 360 c.p.p. se il reperto va incontro a deterioramento o cancellazione*, in *Proc. pen. giust.*, 2013, p. 58.

BRUSCO, C., *La valutazione della prova scientifica*, in *Dir. pen. proc.*, 2008, suppl. al n. 6, p. 27.

BRUTTO, G., *Deep Web: osservazioni pedo support community*, in G. COSTABILE – A. ATTANASIO – M. IANULARDO (a cura di), *IISFA Memberbook 2014. Digital forensics. Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER*, Forlì, 2015.

C

CACCAVELLA, D. E., *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, http://www.marcomattiucci.it/l482008.php, 30 novembre 2015.

CAJANI, F., *Alla ricerca del log (perduto)*, in *Dir. dell'Internet*, 2006, p. 572.

CAJANI, F., *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, http://www.marcomattiucci.it/l482008.php, 30 novembre 2015.

CAJANI, F., *Le operazioni digitali sotto copertura: l'agente provocatore e l'attività di contrasto nelle indagini informatiche*, in S. ATERNO - F. CAJANI- G. COSTABILE - M. MATTIUCCI - G. MAZZARACO (a cura di), *Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Forlì, 2011.

CALAMANDREI, P., *La prova documentale*, Padova, 1997.

CAMON, A., *Le riprese visive come mezzo di indagine: spunti per una riflessione sulle prove incostituzionali*, in *Cass. pen.*, 1999, p. 1211.

CAMPANELLA, S., *Profili problematici in tema di documenti dichiarativi*, in *Ind. Pen.*, 2008, vol. 11, fasc. 1, p. 106.

CANZIO, G., *Prova scientifica, ragionamento probatorio e libero convincimento del giudice*, in *Dir. pen. proc.*, 2003, p. 1194.

CAPPELLETTI, M., *La natura delle norme sulle prove*, in *Riv. it. dir. proc. pen.*, 1969, p. 95.

CAPRIOLI, F., *Colloqui riservati e prova penale*, Torino, 2000.

CAPRIOLI, F., *Riprese visive nel domicilio e intercettazione "per immagini"*, in *Giur. cost.*, 2002, p. 2178.

CARDONA, G.R., *Antropologia della scrittura*, Torino, 2009,

CARLI, L., *Le indagini preliminari nel sistema processuale penale. Accusa e difesa nella ricerca e predisposizione della prova penale*, II ed., Milano, 2005.

CARNELUTTI, F., *Documento e negozio giuridico*, in *Riv. dir. proc. civ.*, 1926, I, p. 105.

CARNELUTTI, F., *La prova civile. Parte generale. Il concetto giuridico della prova*, Milano, rist. 1992.

CARTABIA, M., *Le sentenze "gemelle": diritti fondamentali, fonti, giudici*, in *Giur. cost.*, 2007, p. 3535.

CASEY, E., *Digital Evidence and Computer Crime*, II ed., Elsevier, 2004.

CASEY, E., *Error, uncertainty, and loss in digital evidence*, in *Int. J. Dig. Evidence*, 2002, p. 1.

CATALANO, E. M., voce *Prova (canoni di valutazione della)*, in *Dig. disc. pen.*, agg. II, 2008, p. 794.

CERQUA, F., *Le investigazioni informatiche e la protezione dei dati personali negli Stati Uniti ed in Italia: due modelli a confronto*, in P. CORSO - E. ZANETTI, (a cura di), *Studi in onore di Mario Pisani, II, Diritto processuale penale e profili internazionali: diritto straniero e diritto comparato*, Piacenza, 2010.

CHELO, A., *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, Padova, 2014.

CHELO, A., *Rilievi irripetibili di p.g. o accertamenti tecnici irripetibili?*, in *Dir. pen. proc.*, 2014, 2, p. 209.

CIAVOLA, A., *Prova testimoniale e acquisizione per suo tramite del contenuto delle intercettazioni telefoniche*, in *Cass. pen.*, 2000.

COLAIOCCO, S., *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. pen.*, 1, 2014.

COLOMBO, E., *"Data retention" e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen.*, 7/8, 2014, pag. 2705.

COMOGLIO, L. P., *L'utilizzabilità "assoluta" delle prove "incostituzionali",* in *Riv. dir. proc.*, 2011, p. 30.

COMOGLIO, L. P., *Perquisizione illegittima ed inutilizzabilità derivata delle prove acquisite con il susseguente sequestro*, in *Cass. pen.* 1996, p. 1548;

CONSO, G., *Il concetto e le specie d'invalidità*, Milano, 1972.

CONSO, G., *La natura giuridica delle norme sulla prova nel processo penale*, in *Riv. dir. proc.*, 1970, p. 20.

CONSO, G., – GREVI, V., *Compendio di procedura penale*, Padova, 2010.

CONTE, M. – GEMELLI, M. – LICATA, F., *Le prove penali*, Milano, 2011.

CONTE, M., – LOFORTI, R., *Gli accertamenti tecnici nel processo penale*, Milano, 2006.

CONTI, C., *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007.

CONTI, C., *Al di là di ogni ragionevole dubbio*, in AA.VV., *Novità su impugnazioni penali e regole di giudizio. La legge 20 febbraio 2006*, n. 46, coordinato da A. SCALFATI, Milano, 2006.

CONTI, C., *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali*, in *Cass. pen.*, 2013, vol. 53, fasc. 2, p. 485.

CONTI, C., *Attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, in S. LORUSSO (a cura di), *Le nuove norme sulla sicurezza pubblica*, Padova, 2008.

CONTI, C., *Il processo si apre alla scienza. Considerazioni sul procedimento probatorio e sul giudizio di revisione*, in *Riv. it. dir. proc. pen.*, 2010, pp. 1204.

CONTI, C., *Il volto attuale dell'inutilizzabilità: derive sostanzialistiche e bussola della legalità*, in *Dir. pen. proc.*, pp. 781-797.

CONTI, C., *Intercettazioni e inutilizzabilità: la giurisprudenza aspira al sistema*, in *Cass. pen.*, fasc. 10, 2011, p. 3638.

CONTI, C. - TONINI, P., *Il diritto delle prove penali*, Milano, 2012.

CONTI, C. - TORRE, M., *Spionaggio informatico nell'ambito dei social network*, in AA.VV., *Le indagini atipiche*, (a cura di A. SCALFATI), Torino, 2014.

CONTI, G., - MACCHIA, A., *Indagini preliminari*, in *Enc. giur.*, XVI, Roma, 1989, p. 7.

CORBO, A., *I documenti*, in A. SCALFATI (a cura di), *Le prove*, in *Trattato di procedura penale*, II, diretto da G. SPANGHER, Torino, 2009.

CORDERO, F., *Guida alla procedura penale*, Torino, 1986.
CORDERO, F., *Il procedimento probatorio*, in ID, *Tre studi sulle prove penali*, Milano, 1963.
CORDERO, F., *Procedura penale*, 8ˆ ed., Milano, 2006.
CORDERO, F., *Procedura penale*, Milano, 1971.
CORDERO, F., *sub. art. 234*, in *Codice di procedura penale commentato*, Torino, II ed., 1992.

CORTESI, M. F., *Il Decreto antiterrorismo. I riflessi sul sistema processuale, penitenziario e di prevenzione*, in *Dir. pen. proc.*, 2015, 8, p. 950.

CURTOTTI NAPPI, D., *I rilievi e gli accertamenti sul locus commissi delicti nelle evoluzioni del codice di procedura penale*, in *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze*, a cura di CURTOTTI – SARAVO, Torino, 2013.
CURTOTTI NAPPI, D. - SARAVO, L., *L'approccio multidisciplinare nella gestione della scena del crimine*, in *Dir. pen. proc.*, 2011, 5, p. 623.

D

D'AMBROSIO, L., *Pratica di polizia giudiziaria*, Padova, 2012.
D'AMBROSIO, L., - VIGNA, P. L. *La pratica di polizia giudiziaria, I, La polizia giudiziaria nel processo penale*, VII ed., Padova, 2007.

D'ANDRIA, M., *Un tentativo di definizione degli atti non ripetibili*, in *Cass. pen.*, 1992, p. 1350.

D'ISA, R., *Sulla disciplina dei documenti nel nuovo processo penale*, in *Riv. it. dir. proc. pen.*, 1992, p. 1406.

DAMASKA, M. R., *Il diritto delle prove alla deriva*, Bologna, 2003.

DANIELE, M., *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, p. 440.

DANIELE, M., *La cooperazione giudiziaria. Ricerca e formazione della prova*, in R.E. KOSTORIS (a cura di), *Manuale di procedura penale europea*, Milano, 2014.

DE FLAMMINEIS, S., *Le intercettazioni telematiche*, in *Dir. pen. proc.*, 8, 2013, p. 988.

DE LEO, G., *Le indagini tecniche di polizia: un invito al legislatore*, in *Cass. pen.*, 1996, p. 697.

DELL'ORTO, D., *Pedopornografia online e indagini informatiche. Complessità e peculiarità tecnico-giuridiche della materia*, in *Cass. pen.*, 2007, 3042.

DELL'ANNO, P., *Accertamento e valutazione nelle attività di consulenza disposte dal pubblico ministero*, in *Giust. pen.*, 1991, p. 241.

DI BITONTO, M.L. – VITALE, A., – MACRILLÒ, A. – BARBIERI, A., – FORLANI, E., *La ratifica della Convenzione del Consiglio d'Europa sul Cybercrime: profili processuali*, in *Diritto dell'*Internet, 2008, p. 503.

DI PAOLO, G., *Tecnologie del controllo e prova penale. L'esperienza statunitense e spunti per la comparazione*, Milano, 2008.

DOMINIONI, V., *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005.

DONDI, A., *Paradigmi processuali ed "*expert witness testimony*" nel diritto statunitense*, in *Riv. trim. dir. proc. civ.*, 1996, p. 261.

E - F

FANUELE, C., *Il concetto di privata dimora ai fini delle intercettazioni ambientali*, in *Cass. pen.*, 2001, p. 2746.

FELICIONI, P., *Le ispezioni e le perquisizioni*, in *Trattato di procedura penale*, diretto da G. UBERTIS e G.M. VOENA, Milano, 2012.

FERRARELLA, L., *Tecnologia per la sicurezza, ma tuteliamo anche la privacy*, in *Corriere della Sera*, 9 dicembre 2015.

FERRARIS, M., *Documentalità. Perché è necessario lasciar tracce*, Roma, 2012.

FILIPPI, L., *Il GPS è una prova "incostituzionale"? Domanda provocatoria, ma non troppo, dopo la sentenza Jones della Corte Suprema U.S.A.*, in *Arch. pen.*, 2012, 1.

FILIPPI, L., *L'home watching: documento, prova atipica o prova incostituzionale?*, in *Dir. pen. proc.*, 2001, p. 1395.

FILIPPI, L., *L'intercettazione di comunicazioni*, Milano, 1997, p. 235.

FILIPPI, L., *Le sezioni unite decretano la morte dell'agente segreto attrezzato per il suono*, in *Cass. pen.*, 2004, p. 2094.

FLOR, R., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung*, in *Riv. trim. dir. pen. eco.*, 3, 2009, p. 695.

FLOR, R., *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, www.penalecontemporaneo.it, 30 novembre 2015.

FLOR, R., *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di* Internet, www.penalecontemporaneo.it, 30 novembre 2015.

FLORIAN, E., *Delle prove penali*, III ed., Milano, 1961.

FOSCHINI, G., *Sistema del diritto processuale penale*, I, Milano, 1965.

FRANCESCO, P., *Sui rapporti tra indagini mediante agente provocatore, indagini ordinarie e sequestro probatorio del computer*, in *Dir. pen. proc.*, 2010, 10, p. 1166.

FUMU, G., *sub art. 266-bis c.p.p.* in *Commento al codice di procedura penale*, coordinato da M. CHIAVIARIO, III Agg., Torino, 1990.

G

GABRINI, D., *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, http://www.marcomattiucci.it/l482008.php, 30 novembre 2015.

GAETA, P., *sub art. 360 c.p.p.*, in *Codice di procedura penale commentato*, GIARDA-SPANGHER (a cura di), II, Milano, 2010.

GALANTINI, N., *Considerazioni sul principio di legalità processuale*, in *Cass. pen.*, 1999, p.1989.

GALANTINI, N., *L'inutilizzabilità della prova nel processo penale*, Padova, 1992.

GALANTINI, N., voce *Inutilizzabilità (dir. proc. pen.)*, in *Enc. dir.*, agg., vol. I, Milano, 1997.

GARUTI, G., *Le intercettazioni preventive nella lotta al terrorismo internazionale*, in *Dir. pen. proc.*, 2005, p. 1457.

GIORDANO, P., *Inapplicabili le garanzie dell'intercettazione al semplice monitoraggio della posizione*, in *Guida dir.*, 2002, 23, p. 51.

GIOSTRA, G., *Contraddittorio (principio del): II) diritto processuale penale*, in *Enc. giur. Treccani*, vol. IX, Roma, agg. 2001.

GIRONI, E., *La prova indiziaria*, in AA.VV., *La prova penale*, trattato diretto da A. GAITO, vol. III, Torino, 2008.

GIUNCHEDI, F., *Accertamenti tecnici*, in *Dig. pen.*, V agg., Torino, 2010, p. 1.

GIUNCHEDI, F., *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, Torino, 2009.

GREVI, V., *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost*., 1973, p. 341.

GREVI, V., *Prove*, in G. CONSO - V. GREVI (a cura di), *Compendio di procedura penale*, Padova, 2006.

GREVI, V., NEPPI MODONA, G. P., *Introduzione al progetto preliminare del 1988*, in *Il nuovo codice di procedura penale dalle leggi delega ai decreti delegati*, vol. IV, Padova, 1990.

GRIFANTINI, F. M., voce *Inutilizzabilità*, in *Dir. pen. proc.*, vol. VII, Torino, 1993, p. 249.

GRILLI, L., *Le indagini preliminari della polizia giudiziaria e del pubblico ministero*, Padova, 2012.

GUIDI, P., *Teoria giuridica del documento*, Milano, 1950.

H - I

HANSEN, M., - PFITZMANN, A., *Techniken der Online Durchsuchung: Gebrauch, Missbrauch, Empfehlungen*, in F. ROGGAN (Hrg), *Online Durchsuchungen: Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils*, Bwv Berliner-Wissenchaft, Auflage, 2008.

IACOBACCI, *Sulla necessità di riformare la disciplina delle intercettazioni prendendo le mosse dalle esitazioni applicative già note*, in *Giust. pen.*, 2011, III, p. 365.

IAFISCO, L., *La sentenza penale come mezzo di prova*, Torino, 2002.

IASILLO, A., *Agenti provocatori e sequestro probatorio. Male captum, (non) bene retentum?*, in *Dir. e giust*., 40, 2004, p. 40.

ICHINO, G., *L'attività di polizia giudiziaria*, in AA.VV., *Indagini preliminari ed instaurazione del processo*, a cura di M. G. AIMONETTO, Torino, 1999.

IOVENE, F., *Data retention tra passato e futuro. Ma quale presente?*, in *Cass. pen.*, 12, 2014, p. 4274.

IOVENE, F., *Le c.d. perquisizioni online tra nuovi diritti ed esigenze di accertamento penale*, su www.penalecontemporaneo.it

IOVENE, F., *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale,* in *Riv. trim. diritto penale contemporaneo*, 3-4, 2014, p. 329.

IRTI, N., *Sul concetto giuridico di documento*, in *Norme e fatti*, Milano, 1984.

KOSTORIS, R. E., *I consulenti tecnici nel processo penale*, Milano, 1993.

KOSTORIS, R. E., *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in AA.VV, *Nuove tendenze di giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, L. RUGGERI - L. PICOTTI (a cura di), Torino, 2011, p.180.

L

LARONGA, A., *Il pedinamento satellitare: un atto atipico lesivo di diritti inviolabili?*, in *Quest. giust.*, V, 2002, p. 1155.

LARONGA, A., *L'utilizzabilità probatoria del controllo a distanza eseguito con sistema satellitare g.p.s.*, in *Cass. pen.*, 2002, p. 3058.

LARONGA, A., *Le prove atipiche nel processo penale*, Padova, 2002.

LEONE, G., *Trattato di diritto processuale penale*, II, Napoli, 1961, p. 189.

LOGLI, A., *Commento alla sentenza n. 753/2007*, in *Cass. pen.*, 7-8, 2008, p. 2956.

LONATI, S., *Il contraddittorio nella formazione della prova orale e i principi della CEDU: una proposta de iure condendo*, www.penalecontemporaneo.it, 16 luglio 2012.

LORENZETTO, E., *Le attività urgenti di investigazione informatica,* in *Sistema penale e criminalità informatica*, L. LUPÀRIA (a cura di), Milano, 2009.

LORENZETTO, E., *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenuto al contenitore, passando per la copia*, in *Cass. pen.*, 2010, p. 1533.

LORUSSO, S., *Investigazioni scientifiche, verità processuali ed etica degli esperti*, in *Dir. proc. pen.*, 2010, p. 1345.

LORUSSO, S., *La prova scientifica*, in *La prova penale*, trattato diretto da A. GAITO, Torino, 2008.

LORUSSO, S., *L'arte di ascoltare e l'investigazione penale tra esigenze di giustizia e tutela della privatezza*, in *Dir. pen. proc.*, 2011, 11, p. 1397.

LUBERTO, M. - ZANETTI, G., *Il diritto penale nell'era digitale. Caratteri, concetti e metafore*, in *Indice penale*, 2008, p. 497.

LUPÀRIA, L., *Attività d'indagine a iniziativa della polizia giudiziaria*, in G. GARUTI (a cura di), *Indagini preliminari e udienza preliminare*, in *Trattato di procedura penale*, diretto da G. SPANGHER, vol. III, Torino, 2009, p. 225.

LUPÀRIA, L., *Il caso Vierika: un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali*, in *Dir. int.*, 2006, p. 158.

LUPÀRIA, L., *La ratifica della Convenzione cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. I profili processuali*, in *Dir. pen. proc.*, 2008, p. 718.

LUPÀRIA, L. - ZICCARDI, G., *Investigazione penale e tecnologica informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007.

M

MAFFEI, S., *Ipnosi, poligrafo, narcoanalisi, risonanza magentica: metodi affidabili per la ricerca processuale della verità?*, in DE CATALDO NEUBERGER (a cura di), *La prova scientifica nel processo penale*, Padova, 2007.

MAGOULÈS, F., *Fundamentals of Grid Computing: Theory, Algorithms and Technologies*, U.S.A., 2010.

MAIOLI, C. - SANGUEDOLCE, E., *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, www.altalex.com, 30 novembre 2015.

MALINVERNI, A., *Documento: b) diritto penale*, in *ED*, XIII, Milano, 1964.

MANCUSO, E. M, *L'acquisizione di contenuti e-mail*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014.

MANZINI, V., *Istituzioni di diritto processuale penale*, Padova, 1954.

MANZIONE, D., *L'attività del pubblico ministero*. *Indagini preliminari e instaurazione del processo,* coordinato da M. G. AIMONETTO, in *Giurisprudenza sistematica di diritto processuale penale*, diretta da M. CHIAVARIO e E. MARZADURI, Torino, 2009.

MARANDOLA, A., *I registri del pubblico ministero tra notizia di reato ed effetti procedimentali*, Padova, 2001.

MARCOLINI, S., *Le cosiddette perquisizioni online (o perquisizioni elettroniche)*, in *Cass. pen.*, 07/08, 2010, p. 2855.

MARCOLINI, S., *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2, 2015, p. 760.

MARINELLI, C., *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007.

MARINELLI, C., *Intercettazioni processuali e nuovi mezzi di ricerca della prova nell'attività di polizia giudiziaria: videosorveglianza, pedinamento e localizzazione satellitare*, in *Riv. polizia*, 2007, p. 672.

MARINELLI, C., *L'attività dell'agente provocatore per il contrasto alla pedopornografia: "straripamenti" investigativi e relative implicazioni processuali*, in *Cass. pen.*, 2005, p. 2683.

MARINELLI, C., *Le "intercettazioni di immagini" tra questioni interpretative e limiti costituzionali*, in *Dir. pen. proc.*, 1998, p. 1270.

MASSA, M., *La "sostanza" della giurisprudenza europea sulle leggi retroattive*, in *Giur. cost.*, 2009, p. 4657.

MATTIUCCI, M., *Intercettazioni digitali*, www.marcomattiucci.it.

MATTIUCCI, M. – DELFINIS, G., *Forensics Computing*, in *Rass. Arma Carab.*, 2006, p. 62.

MAZZA, O., *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*¸ Relazione al convegno di studi su "Garanzia dei diritti fondamentali e processo penale" organizzato da Diritto penale contemporaneo, Magistratura Democratica e la Camera Penale di Milano il 9 e 10 novembre 2012 presso l'Aula Magna del Palazzo di Giustizia di Milano, reperibile in *www.penalecontemporaneo.it*.

MAZZA, O., *Le deroghe costituzionali al contraddittorio per la prova*, in G. CONSO (a cura di), *Il diritto processuale penale nella giurisprudenza costituzionale*, Napoli, 2006.

MELL, P., GRANCE, T., *The NIST Definition of Cloud Computing*, NIST, Special Publication 800-145, Settembre 2011.

MINNITI, F., *Ricerca CeMISS C8/Z. Le fonti informative e l'open source*, www. difesa.it/SMD_/CASD/IM/CeMISS/Pubblicazioni/Documents/42175_Minniti_0p df.pdf.

MOLINARI, F. M., *Dubbio sull'attendibilità della chiamata in correità ed attribuzione alla stessa di un valore indiziante*, in *Cass. pen.*, 1996, p. 1918.

MOLINARI, F. M., *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, p. 1261.

MOLINARI, F. M., *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2012, p. 697.

MONTI, A., *Attendibilità dei sistemi di computer forensic*, http://www.ictlex.net/?p=287, 30 novembre 2015.

MONTI, A., *No ai sequestri indiscriminati di computer*, in *Diritto dell'Internet*, 3, 2007, p. 268.

MORGIGNI, A., *L'attività di polizia giudiziaria*, Milano, 2002.

MOSCARINI, P., *Art. 184 c.p.p.*, in AA.VV., *Commentario breve al codice di procedura penale*, a cura di G. CONSO E V. GREVI, Padova, 1987.

MOSCARINI, P., *Ispezioni (dir. proc. pen.)*, in *Enc. dir.*, Agg., II, Milano, 1998, p. 465.

MUCCIARELLI, F., *sub art. 4 L. 23 febbraio 1993 N.547 (Criminalità informatica)*, in *LP.* 1996, p. 98.

N

NOBILI, M., *La nuova procedura penale. Lezione agli studenti*, Bologna, 1989.

NOBILI, M., *sub. art. 189 c.p.p.*, in M. CHIAVARIO (coordinato da), *Commento al nuovo codice di procedura penale*, vol. II, Torino, 1990, p. 398

NOVARIO, F., *Criminalità informatica e sequestro probatorio: le modifiche introdotte dalla l. 18 marzo 2008, n. 48 al codice di procedura penale*, in *Riv. dir. proc.*, 2008, p. 1070.

NOVARIO, F., *Le prove informatiche nel processo civile*, Torino, 2014.

O

OLIVIERI, R., *I sistemi di geolocalizzazione e l'analisi forense degli smartphone*, in G. COSTABILE – A. ATTANASIO – M. IANULARDO (a cura di), *IISFA Memberbook 2014. Digital forensics. Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER*, Forlì, 2015.

ONG, W.J., *Oralità e scrittura. Le tecnologie della parola*, Bologna, 1986.

ORLANDI, R., *Atti e informazioni dell'autorità amministrativa nel processo penale. Contributo allo studio delle prove extracostituite*, Milano, 1992.

ORLANDI, R., *Questioni attuali in tema di processo ed informatica*, in *Riv. dir. proc.*, 2009, p. 135.

P

PANSINI, C., *E' valida la prova atipica senza la preventiva audizione delle parti?*, in *Dir. pen. proc.*, 1997, p.1257.

PERCHINUNNO, V., *I mezzi di ricerca della prova*, in *Manuale di procedura penale*, Bologna, 2002.

PERCHINUNNO, V., *Prova documentale: b) diritto processuale penale*, in *Enc. dir.*, XXXVII, Milano, 1988, p. 722.

PERETOLI, P., *Controllo satellitare con G.P.S.: pedinamento o intercettazione?*, in *Dir. pen. proc.*, 2003, I, p. 96.

PERRI, P., *Profili informatico-giuridici della diffusione, mediante strumenti telematici, di materiale pedopornografico*, in *Cass. pen.*, 9, 2008, p. 3466.

PEYRON, C., *Ispezione giudiziale (dir. proc. pen.)*, in *Enc. dir.*, XXII, Milano, 1972, p. 962.

PICA, G., *Diritto penale delle tecnologie informatiche*, Torino, 1999.

PICOTTI, L., *Ratifica della Convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'Internet*, 2008, p. 437.

PINELLI, C., *Sul trattamento giurisdizionale della CEDU e delle leggi con essa confliggenti*, in *Rivista AIC*, marzo 2008.

PITTARO P., - SPANGHER, G., *Le norme contro la pedofilia*, in *Dir. pen. proc.*, 1998, 1222.

POPPER, K. R., *Logica della scoperta scientifica*, Torino, 1970.

PROCACCINO, A., *Prove atipiche*, in A. GAITO (a cura di), *La prova penale*, vol. I, Torino, 2009.

Q – R

RAFARACI, *Ricognizione informale dell'imputato e (pretesa) fungibilità delle forme probatorie*, in *Cass. pen.*, 1998, p. 1745.

REITANO, L., *Esplorare Internet. Manuale di investigazioni digitali e Open Source Intelligence*, Bologna, 2014.

RICCI, A. E., *Digital evidence e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc.*, 2010, 3, p. 337.

RICCI, F., voce *Documento informatico*, in *Il diritto, Enc. de Il Sole-24 Ore*, Milano, 2007, IV, p. 548.

RICCI, G. F., *Le prove atipiche*, Milano, 1999.

RICCIO, G., *Presentazione*, in A. FURGIUELE, *La prova per il giudizio nel processo penale*, Torino, 2007, p. 12.

RIVELLO, P. P., *La prova scientifica*, Milano, 2014.

RIVELLO, P. P., *La struttura, la documentazione e la traduzione degli atti*, in G. UBERTIS E M.G. VOENA (a cura di), *Trattato di procedura penale*, X.1, Milano, 2004.

ROMEO, G., *Le Sezioni unite sull'applicabilità delle disposizioni relative alle intercettazioni alla sottoposizione a controllo e all'acquisizione probatoria della corrispondenza epistolare del detenuto*, in www.penalecontemporaneo.it.

RUOTOLO, G. M., *Hey! You! Get off my cloud!*, in *Archivio penale*, settembre-dicembre 2013, fasc. 3, p. 857.

RUSSO, L., *Le operazioni sotto copertura e le attività di contrasto in materia di delitti sessuali o per la tutela dei minori*, in *Giur. mer.*, 12, 2008, p. 3346.

RUSSO V., – ABET, A., *La prova indiziaria e il "giusto processo". L'art. 192 c.p.p. e la legge 63/2001*, Napoli, 2001.

S

SARTOR, G. *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, Torino, 2012.

SCALFATI, A., *Gli accertamenti tecnici dell'accusa*, in *Indice pen.*, 1992, p. 129.

SCALFATI, A., *La deriva scientista dell'accertamento penale*, in *Proc. pen. giust.*, 2011, n. 5, p. 148.

SCELLA, A., *Brevi riflessioni in tema di accertamenti tecnici, rilievi e tutela del diritto di difesa*, in *Cass. pen.*, 1990, p. 278.

SCOGNAMIGLIO, P., *Criminalità informatica. Commento organico alla Legge 18 marzo 2008, n. 48*, Napoli, 2008.

SERRANI, A., *Sorveglianza satellitare GPS: un'attività investigativa ancora in cerca di garanzie*, in *Arch. pen.*, 2013, 3.

SIGNORATO, S., *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.*, 2012, p. 586.

SIRACUSANO, F., *Manuale di procedura penale*, Milano, 1990, p. 373.

SOTTANI, S., *Rilievi e accertamenti sulla scena del crimine*, in *Arch. pen.*, 2011, 3, 1.

SPANGHER, G., *"E pur si muove": dal male captum bene retentum alle exclusionary rules,* in *Giur. cost.*, 2001, p. 2821.

SPANGHER, G., *La pratica del processo penale, Indagini preliminari e udienza preliminare. Il giudizio. Il procedimento davanti al Tribunale in composizione nonocratica,* vol. II, Padova. 2012.

STRAMAGLIA, M., *Il pedinamento satellitare: ricerca ed uso di una prova "atipica"*, in *Dir. pen. proc.*, 2011, p.

T

TABASCO, G., *Prove non disciplinate dalla legge nel processo penale, Le "prove atipiche" tra teoria e prassi*, Napoli, 2011.

TAMIETTI, A., *L'utilizzazione di prove assunte in violazione di un diritto garantito dalla Convenzione non viola l'equo processo: riflessioni sul ruolo della Corte europea e sulla natura del sindacato da essa operato in margine alla sentenza P.G. e J.H. c. Regno Unito*, in *Cass. pen.*, 2002, p. 1837.

TARUFFO, M., *La prova dei fatti giuridici. Nozioni generali*, Milano, 1992.

TARUFFO, M., *Prove atipiche e convincimento del giudice*, in *Riv. dir. proc.*, 1973, p. 395.

TESTAGUZZA, A., *I sistemi di controllo remoto: fra normativa e prassi*, in *Dir. Proc. Pen.*, 6, 2014, p. 762.

TONINI, P., *Dalla perizia "prova neutra" al contraddittorio sulla scienza*, in *Dir. pen. proc.*, 2011, p. 11.

TONINI, P., *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, p. 401.

TONINI, P., *Il documento informatico: problematiche civilistiche e penalistiche a confronto*, in *Dir. pen. proc.*, 2012, p. 435.

TONINI, P., *Informazioni genetiche e processo penale ad un anno dalla legge*, in *Dir. pen. proc.*, 2010, pp. 883 e ss.

TONINI, P., *La prova penale*, 4ª ed., Padova, 2000.

TONINI, P., *La prova scientifica*, in *Trattato di procedura penale*, AA.VV., diretto a G. SPANGHER, vol. II, t. 1, *Le prove*, a cura di A. SCALFATI, Torino, 2009.

TONINI, P., *Manuale di procedura penale*, XVI ed., Milano, 2015.

TONINI, P., *Nuovi profili processuali del documento informatico,* in *Scienza e processo penale: linee guida per l'acquisizione della prova scientifica*, a cura di L. DE CATALDO NEUBURGER, Padova, 2000.

TONINI, P., *Problemi insoluti della prova documentale*, in *Dir. pen. proc.*, 1996, p. 482.

TONINI, P., *Progresso tecnologico, prova scientifica e contraddittorio*, in *La prova scientifica nel processo penale*, a cura di L. DE CATALDO NEUBURGER, Padova, 2007.

TONINI, P. – CONTI, C., *Il diritto delle prove penali*, Milano, 2012.

TONIUTTI, *Terrorismo, Orlando: "Intercettazioni anche su chat e PlayStation"*, www.repubblica.it, 26 novembre 2015.

TRANCHINA, G., *Le attività della polizia giudiziaria nel procedimento per le indagini preliminari*, in D. SIRACUSANO – A. GALATI – E. ZAPPALÀ (a cura di), *Diritto processuale penale*, II, Milano, 2011.

TROGU, M., *Sorveglianza e "perquisizioni" on-line su materiale informatico*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, p. 431.

U

UBERTIS, G., *Documenti e oralità nel nuovo processo penale* (1991), in ID., *Sisifo e Penelope. Il nuovo codice di procedura penale dal progetto preliminare alla ricostruzione del sistema*, Torino, 1993.

UBERTIS, G., *Documenti e oralità nel nuovo processo*, in *Studi in onore di Giuliano Vassalli*, a cura di M.C. BASSIOUNI - A.R. LA TAGLIATA - A.M. STILE, II, Milano, 1991.

UBERTIS, G., *Prova e contraddittorio*, in *Cass. pen.*, 2002, p. 1182.

UBERTIS, G., *Sistema multilivello dei diritti fondamentali e prospettiva abolizionista del processo contumaciale*, in *Giur. cost.*, 2009, p. 4747.

UBERTIS, G., *Variazioni sul tema dei documenti*, in *Cass. pen.*, 1992, p. 2516.

V

VACIAGO, G., *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, 2012.

VACIAGO, G., *Privacy e tutela dell'ordine pubblico in Europa e negli Stati Uniti: un differente approccio per raggiungere un difficile compromesso*, in *Informatica e diritto*, vol. XVIII, 2009, n. 1, p. 135.

VACIAGO, G., *Profili processuali delle indagini informatiche*, in G. CASSANO – G. SCORZA – G. VACIAGO (a cura di), *Diritto dell'*Internet. *Manuale operativo. Casi, legislazione, giurisprudenza,* Padova, 2013.

VASSALLI, G., *La libertà personale nel sistema delle libertà costituzionali,* in Id., *Scritti giuridici*, vol. III, Milano, 1997, p.177 e ss.

VASSALLI, G., *La protezione della sfera della personalità nell'era della tecnica*, in AA.VV., *Studi in onore di Emilio Betti*, vol. V, Milano, 1962.

VELANI, L.G., *Nuove tecnologie e prova penale: il sistema di individuazione satellitare g.p.s.*, in *Giur. it.*, 2003, p. 2372.

VENTURA, N., *Le investigazioni under cover della polizia giudiziaria*, Bari, 2008.

VESSICHELLI, M., *Sulla possibilità della p.g. di effettuare di propria iniziativa raffronti tra impronte digitali,* in *Cass. pen.*, 1992, p. 689.

VIGNA, P. L., *Elementi di procedura penale per la polizia giudiziaria*, Roma, 2010.

VIGNA, P. L., *La pratica di polizia giudiziaria, I, La polizia giudiziaria nel processo penale*, VII ed., Padova, 2007.

VIGNA, P. L., *Pratica di polizia giudiziaria*, Padova, 2012.

VITALE, A., *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. int.*, 2008, 5, p. 509.

VOENA, G.P., *Atti*, in *Compendio di procedura penale*, diretto da G. CONSO - V. GREVI, Padova, 2010.

VOLLI, U., *Il nuovo libro della comunicazione. Che cosa significa comunicare: idee, tecnologie, strumenti, modelli*, Milano, 2007

Z

ZACCHÉ, F., *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.*, 2013, n. 4, p. 106.

ZACCHÉ, F., *La prova documentale*, in *Trattato di procedura penale*, (diretto da) G. UBERTIS e G.P. VOENA, XIX ed., Milano, 2012.

ZAPPALÀ, E., *Il principio di tassatività dei mezzi di prova nel processo penale*, Milano, 1982.

ZAZA, C., *Il ragionevole dubbio nella logica della prova penale*, Milano, 2008.

ZICCARDI, G., *Informatica giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni digitali*, Tomo II, Seconda ed., Milano, 2012.

ZICCARDI, G., *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in AA.VV., *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime*, a cura di L. LUPÀRIA, Milano, 2009.

ZICCARDI, G., *Le tecniche informatico-giuridiche di investigazione digitale*, in LUPARIA-ZICCARDI (a cura di), *Investigazione penale e tecnologia informatica*, Milano, 2007.

ZICCARDI, G., *Manuale breve di informatica giuridica*, Milano, 2008, p. 205.

ZINGARELLI, N., *sub pedinare*, in M. CANNELLA – B. LAZZARINI (a cura di), *Lo Zingarelli 2015. Vocabolario della lingua italiana*, 2015, p. 1357.

ZÖLLER, V., *Die Vorratsspeicherung von Telekommunikationsdaten – (Deutschen) Wege und Irrwege, Congress on the Criminal Law Reforms* in *The World and in Turkey*, Atti

del convegno internazionale svoltosi a Istanbul-Ankara dal 26 maggio al 4 giugno 2010, Istanbul, 2010.

RINGRAZIAMENTI

Il primo pensiero al mio Maestro, il prof. Paolo Tonini, non solo per il prezioso aiuto nella ricerca, ma anche per aver creduto in me, dall'inizio sino alla fine di questo meraviglioso percorso. A lui, quindi, infinite grazie per il supporto, le pazienti revisioni, le gradite opportunità didattiche. Credo che esistano differenti modi di svolgere un corso di dottorato, credo anche che il migliore di questi sia guardare al percorso, prima ancora che alla meta: questo è il suo migliore insegnamento ed io ne farò tesoro.

Grazie alla scuola fiorentina, della quale adesso mi onoro di far parte: un "laboratorio di idee" frutto di una condivisione continua di opinioni. Nulla è più stimolante.

A Martina devo la cosa più importante, una incondizionata e rara fiducia che mi ha spronato nei momenti di difficoltà. Niente è più gratificante.

Ai miei genitori, invece, devo quello che sono, e per questo non potrò mai ringraziarli abbastanza.

Alla piccola Mia, infine, il mio ultimo pensiero: è stata la mia maggiore distrazione, ma mi ha reso un uomo migliore, e questo non ha prezzo.