UNIVERSITÀ DEGLI STUDI DI PAVIA

Dipartimento di Giurisprudenza

Dottorato in Diritto pubblico, giustizia penale e internazionale
XXIX ciclo

Prova informatica e processo penale

Relatore:

Chiar. mo Prof. Paolo Renon

Tesi di dottorato di

Severino Murgia

CAPITOLO I

IL RUOLO DELLA PROVA SCIENTIFICA NEL PROCESSO PENALE

CAPITOLO II

LA DEFINIZIONE DI PROVA DI CARATTERE INFORMATICO

CAPITOLO III

PROVA INFORMATICA E DIRITTI FONDAMENTALI DELLA PERSONA

CAPITOLO IV

LE PROVE INFORMATICHE DI CARATTERE "TIPICO"

CAPITOLO V

LE PROVE INFORMATICHE DI CARATTERE "ATIPICO"

Introduzione

Il tema del presente lavoro prende le mosse dall'ormai inarrestabile espansione dell'informatica nella vita quotidiana di ciascuno. Tale fenomeno risulta di estrema rilevanza per il processo penale, in quanto gli strumenti elettronici sono in grado di registrare un numero elevatissimo di informazioni che possono rivelarsi estremamente utili all'interno dello stesso. Tuttavia, l'introduzione, tra gli strumenti conoscitivi del giudice, degli elementi probatori di carattere digitale si caratterizza per essere estremamente problematica sotto molteplici punti di vista. La prima difficoltà deriva dalla stessa natura della prova informatica, la quale, inserendosi nella più ampia categoria delle prove scientifiche, porta con sé tutte le problematiche a quest'ultima connesse, in relazione tanto al momento acquisitivo quanto a quello valutativo.

La prospettiva abbracciata dall'elaborato è stata quella per cui la *digital forensics* non costituisca un'utile risorsa soltanto in relazione a quei procedimenti aventi per oggetto i c.d. *computer crimes*, dovendo, viceversa, riconoscersi l'importanza che queste tipologie di prove possono acquistare in qualsiasi processo penale.

Una delle esigenze cui si è tentato di dare una risposta è stata quella di fornire un'organizzazione organica della materia che si contrapponesse alla costante frammentarietà degli interventi di carattere legislativo. Infatti la l. 18 marzo 2008, n. 48, con la quale è stata data ratifica alla Convenzione di Budapest sul *cybercrime*, pur contenendo numerosi spunti interessanti per quanto attiene alla formazione e all'utilizzazione di prove di carattere digitale, si è limitata ad interpolare il codice di rito penale, evitando di affrontare in maniera sistematica la questione dello statuto processuale delle prove di stampo informatico.

Per questo motivo, si è immediatamente posta la questione di individuare, come primo punto fermo della trattazione, una definizione di prova informatica che fosse valida sia da una prospettiva sia tecnico-scientifica sia giuridica. Muovendosi in tale direzione si è, innanzitutto, avuto modo di delineare, in relazione alle modalità di raccolta degli elementi probatori, due macrocategorie di prove informatiche: da un lato, quelle c.d. statiche, corrispondenti a quell'insieme di dati informatici memorizzati stabilmente su di un elaboratore elettronico e, dall'altro lato, quegli strumenti che permettono l'acquisizione di dati che circolano all'interno delle reti informatiche come *Internet*.

Sempre partendo dalla considerazione circa l'importanza che l'elettronica di consumo ha raggiunto nella vita quotidiana di ciascun individuo, si è avuto modo di sottolineare come le operazioni di *digital forensics* non siano indifferenti per quanto riguarda la tutela dei diritti fondamentali dell'uomo. Infatti ormai chiunque affida al proprio *smartphone*, *laptop* o altro *device* elettronico un gran numero di informazioni, molte delle quali di carattere personalissimo, verso le quali non può non immaginarsi una qualche forma di tutela. In relazione a ciò, i beni giuridici che maggiormente rischiano di essere compressi dalla raccolta di materiale probatorio di stampo elettronico sono stati individuati nel diritto alla riservatezza, in quello dell'inviolabilità del domicilio e, infine, in quello alla libertà e segretezza delle comunicazioni. Queste posizioni giuridiche soggettive sono, attualmente, tutelate, come è noto, da un ampio sistema multilivello di garanzie che trovano espressione non solo nella nostra Costituzione ma, oggi, anche nella Convenzione europea dei diritti dell'uomo e nel diritto dell'Unione europea.

In questa prospettiva, quello che si è cercato di evidenziare maggiormente è l'imprescindibile ruolo che svolge il rispetto della doppia riserva di legge e di giurisdizione, nella

ricerca di un equilibrato bilanciamento tra le opposte esigenze che vengono in gioco nel settore. Infatti, alla luce dell'importanza che rivestono all'interno della Costituzione, della C.e.d.u. e del diritto dell'Unione europea i beni giuridici citati, si è tentato di sottolineare come soltanto la legge, in quanto provvedimento di carattere generale ed astratto, emanato dal Parlamento ed affidato per la sua applicazione alla magistratura, possa definire presupposti, forme e limiti di un'attività potenzialmente idonea a comprimere tali diritti al fine di perseguire gli obiettivi propri del processo penale, ossia l'accertamento in merito alla responsabilità o meno per il fatto di reato da parte dell'imputato.

Una volta delineati i confini dei diritti fondamentali rilevanti in relazione alle operazioni di raccolta di elementi probatori di stampo elettronico, si è ripreso il discorso andando a effettuare un'analisi più puntuale dei singoli istituti processuali che permettono l'ingresso nel processo penale di dati informatici. In tal senso, è stato scelto di trattare in primo luogo i mezzi di ricerca della prova regolati espressamente dal codice di rito penale. In secondo luogo, lo studio è proseguito avendo come punto di riferimento le prove di carattere atipico, le quali rappresentano sotto certi aspetti il momento di maggior tensione tra le esigenze di accertamento dei fatti e la tutela dei diritti dei singoli.

Capitolo I

Il ruolo della prova scientifica nel processo penale

SOMMARIO: 1. Introduzione alla prova scientifica – 2. La prova scientifica nella normativa processuale penale italiana – 3. La valutazione della prova scientifica

1. Introduzione alla prova scientifica

Con l'espressione «prova scientifica» si fa generalmente riferimento all'utilizzo, all'interno del processo, di conoscenze di carattere scientifico, al fine di poter dimostrare la verità di un determinato enunciato fattuale[1]. Più precisamente, intendendo il termine prova come risultato di prova[2], alcuni Autori giungono ad affermare che per prova scientifica si deve intendere la formazione del convincimento del giudice circa la sussistenza o meno di un determinato fatto sulla base di conoscenze che non sono proprie dell'uomo comune, ma che

[1] La definizione è di M. TARUFFO, *Prova scientifica (diritto processuale civile)*, in *Enc. dir.*, ann. II, t. I, pp. 965 s. La connessione tra processo e scienza è risalente. Volendo cercare un punto di partenza, si può affermare che il problema dell'ingresso della scienza nel processo nasce col divieto di utilizzazione delle ordalie nel processo. Infatti, con tale provvedimento, il processo acquista un contenuto di carattere storico; diventa necessario, in altri termini, accertare dei fatti per poi qualificarli giuridicamente. Nel momento in cui si pone la questione della ricostruzione di un fatto, emerge anche la problematica legata all'utilizzo di strumenti di carattere scientifico nel processo. Per alcuni spunti in tal senso, v. F. CORDERO, *Procedura penale*, Giuffrè, Milano, 9° ed., 2012, pp. 781 ss.

[2] Cfr. V. DENTI, *Scientificità della prova e libera valutazione del giudice*, in *Riv. dir. proc.*, 1972, p. 414, per il quale il termine prova può essere inteso in tre diverse accezioni. Secondo la prima di queste, la prova è da intendere come il mezzo che si utilizza – testimonianza, documento, perizia – per dimostrare il *thema probandum*. Da un diverso punto di vista, ci si può riferire alla prova come al procedimento che le parti ed il giudice pongono in essere per acquisire al processo un certo mezzo di prova. Infine, la prova può essere anche intesa come il risultato del procedimento probatorio, quindi il convincimento raggiunto dal giudice circa la verità o la falsità di un certo enunciato.

trascendono il patrimonio di nozioni dello stesso[3]. Recentemente, l'argomento è stato oggetto di nuove riflessioni sia da parte della dottrina sia da parte della giurisprudenza italiana. La ragione del rinnovato interesse per la materia va ricercata oltre che in alcune importanti pronunce della giurisprudenza statunitense sul tema[4], soprattutto in due fattori di carattere non prettamente giuridico.

Il primo, di natura tecnologica, è rappresentato dallo sviluppo della scienza, la quale ha permesso la messa a punto di nuove e più sofisticate tecniche di indagine. Queste consentono, da un lato, una migliore ricognizione del fatto che si intende provare; dall'altro lato, rendono solo ora possibile la prova di certi fatti che precedentemente o, non venivano accertati oppure, venivano provati sulla base del senso comune[5].

L'altro fattore, di tipo culturale, che ha contribuito a ridestare l'interesse per la prova scientifica è dato dall'allargamento del concetto di scienza[6]. Secondo una visione classica

[3] Questa è la definizione accettata da V. DENTI, *op. cit.*, p. 421. O. DOMINIONI, in *Prova scientifica (diritto processuale penale)*, in *Enc. dir.*, ann. II, t. I, p. 977, dà una lettura estensiva di tale definizione alla luce dell'art. 220 c.p.p. Secondo l'Autore la locuzione si riferisce a tutti quei mezzi di prova nei quali si utilizzano metodologie tecnico-scientifiche che richiedono particolare competenze.

[4] Ci si riferisce principalmente alla nota sentenza *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 US 579 (1993) trad. it. a cura di A. DONDI, *Paradigmi processuali ed* "expert testimony" *nel diritto statunitense*, in *Riv. trim. dir. proc. civ.*, 1996, pp. 277 ss.

[5] Un esempio è offerto da P. TONINI, *La Cassazione accoglie i criteri* Daubert *sulla prova scientifica. Riflessi sulla verifica delle massime d'esperienza*, in *Dir. pen. proc.*, 2011, p. 1347, il quale fa riferimento alla sentenza del giudice dell'udienza preliminare di Vigevano sull'omicidio di Chiara Poggi. In quella sede ci si interrogò sulla verosimiglianza delle dichiarazioni dell'imputato circa il tragitto che egli avrebbe compiuto dalla porta di ingresso alle scale dell'abitazione della vittima senza sporcarsi le scarpe, nonostante il pavimento fosse pieno di macchie di sangue. Ad avviso del pubblico ministero, tale versione era altamente inverosimile. Il punto di partenza della pubblica accusa era costituito dalla massima d'esperienza per cui un uomo che deve andare dal punto A al punto B sceglierà sempre la via più breve. Se questa affermazione è vera, allora ne segue che difficilmente l'imputato sarebbe potuto entrare nell'appartamento senza calpestare almeno una delle macchie di sangue. Il giudice dell'udienza preliminare di Vigevano, però, non si fermò a questa massima di comune esperienza. Infatti, decise di nominare un perito affinché calcolasse la probabilità che taluno, muovendosi in quel determinato ambiente potesse evitare di sporcarsi le scarpe. Il perito realizzò un esperimento, utilizzando un finto pavimento macchiato di sangue e chiedendo ad alcuni sperimentatori di correre da un punto ad un altro. Il risultato fu che nessuno di costoro calpestò alcuna macchia di sangue. In questa maniera, l'asserto del pubblico ministero, basato su massime d'esperienza, fu smentito sulla base di un esperimento scientifico.

[6] In tal senso, M. TARUFFO, *op. cit.*, pp. 967 s.

della scienza, questa comprendeva solo le c.d. scienze dure come la fisica, la chimica, la biologia. In altri termini, solo le discipline di carattere empirico potevano definirsi scienza. Ormai, invece, si ammette anche l'esistenza delle scienze c.d. sociali, come la psicologia, la sociologia, l'economia o l'antropologia[7]. Evidentemente, la ricostruzione del concetto di scienza non è indifferente per quanto riguarda l'attività giurisdizionale. Infatti se la scienza è confinata all'àmbito delle scienze dure, allora il giudice potrà far ricorso a massime d'esperienza o al senso comune tutte le volte in cui dovrà risolvere una questione attinente alle materie interessate dalle scienze sociali. Viceversa, nel momento in cui si riconosce piena dignità scientifica anche a materie diverse dalla scienza empirica, allora aumentano gli spazi per le prove scientifiche.

Accanto ai fenomeni sommariamente descritti, il tema della prova scientifica è stato nuovamente oggetto di dibattito tra gli studiosi del processo penale, grazie anche ad alcune pronunce della giurisprudenza nordamericana. Questi arresti giurisprudenziali, a causa della loro forza persuasiva, sono stati recepiti anche da una parte della giurisprudenza italiana e hanno costituito oggetto di approfondimenti da parte della dottrina del nostro Paese[8]. Per questo motivo, appare necessario effettuare una breve digressione sul tema.

[7] M. TARUFFO, *Le prove scientifiche nella recente esperienza statunitense*, in *Riv. trim. dir. proc. civ.*, 1996, pp. 230 ss. fa riferimento al concetto di *social science evidence* nella giurisprudenza nordamericana. Con l'espressione ci si riferisce ai casi in cui il giudice per valutare taluni elementi della fattispecie, come quello dell'osceno, faccia riferimento non a massime d'esperienza, ma a studi sociologici sul tema.

[8] V. le motivazioni di Cass. sez. IV, 17 settembre 2010, Cozzini ed altri, in *Dir. pen. proc.*, 2011, pp. 1341 ss. e di Cass. sez. IV, 29 gennaio 2013, Cantore, in *Cass. c.e.d.* n. 255105. In dottrina, si riscontra un consenso pressoché unanime sull'importanza dei criteri di ammissione della prova scientifica elaborati dalla Corte suprema degli Stati Uniti d'America, *ex multis*, F. CAPRIOLI, Scientific evidence *e logiche del probabile nel processo per il "delitto di Cogne"*, in *Cass. pen.*, 2009, p. 1869; C. CONTI, Iudex peritus peritorum *e ruolo degli esperti nel processo penale*, in *La prova scientifica nel processo penale*, a cura di P. Tonini, Ipsoa, Milano, 2008, p. 34. Pur riconoscendone la centralità per il dibattito sul tema, O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005, pp. 138 s. e P. P. RIVELLO, *La prova scientifica*, Giuffrè, Milano, 2014, pp. 80 ss. non mancano di sottolineare alcune delle criticità sottese agli approdi cui si fa riferimento.

Il punto di partenza è rappresentato dalla pronuncia della *Court of appeals of District of Columbia, Frye v. United States*[9]. In quel processo era stata chiesto di ammettere, attraverso una *expert testimony*, l'impiego ai fini di prova, di una delle prime macchine della verità. L'esperto di cui si chiedeva l'ammissione sosteneva che attraverso l'analisi della pressione sanguigna fosse in grado di capire se le risposte che l'imputato dava all'interrogante fossero sincere o meno[10]. Lo strumento richiesto costituiva al tempo un ritrovato tecnologico particolarmente avanzato e ancora poco diffuso[11]. Per questo motivo, la valutazione cui era chiamata la Corte era particolarmente complessa. Ovviamente, per risolvere la questione concreta dell'ammissibilità della prova era necessario individuare un criterio di carattere generale che potesse orientare la scelta del giudice. Si trattava, in sostanza, di trovare un parametro che fosse in grado di distinguere tra le tecniche che, per quanto nuove ed avanzate, fossero nondimeno scientifiche e quelle che, invece, fossero esclusivamente parascientifiche e che, quindi, non avrebbero mai potuto fornire al giudice elementi utili per la propria decisione. A parere dei giudici, la verifica dell'adesione alla metodologia scientifica del mezzo di prova che si voleva usare doveva basarsi sulla generale accettazione del metodo proposto

[9] *Frye v. United States*, 293 F. (D.C.) 1013 (1923). Prima di questa pronuncia, il criterio di ammissione per l'*expert witness* era rappresentato dal *commercial marketplace test*. L'affidabilità dell'esperto era vagliata alla luce del successo riscosso dallo stesso nel proprio mercato di riferimento. Più un determinato professionista era rinomato nel proprio campo, maggiore era la sua credibilità. Come si nota, l'attenzione è posta più sull'attendibilità dell'esperto che non sull'affidabilità del metodo o della tecnica utilizzata. Per alcune indicazioni bibliografiche sul punto, v. O DOMINIONI, *La prova penale*, cit., p. 116, nt. 2.

[10] Per espressa previsione legislativa un tale metodo non sarebbe in alcun modo ammissibile nel nostro processo penale. Infatti, l'art. 188 c.p.p., riprendendo quanto previsto dall'art. 64, co. 2° c.p.p. in tema di interrogatorio dell'indagato, vieta l'utilizzo di tecniche che possano inficiare la capacità di autodeterminazione della persona. Tra questi strumenti, la dottrina riconduce pacificamente anche il poligrafo; v., tra i tanti, V. GREVI, *Prove*, in *Compendio di procedura penale*, a cura di G. Conso, V. Grevi, M. Bargis, Cedam, Padova, 8° ed., 2014, p. 293.

[11] Un'altra motivazione che spinse i giudici nell'elaborazione di un nuovo *test* di ammissibilità della *expert testimony* era rappresentata dall'inapplicabilità al caso concreto del *commercial marketplace test*. Infatti, non esisteva alcun mercato di riferimento per i *lie detector* e, quindi, era impossibile valutare la credibilità dell'esperto sulla base del suo successo commerciale. In tal senso, DAVID L. FAIGMAN, DAVID H. KAYE, MICHAEL J. SAKS & JOSEPH SANDERS, *Modern Scientific Evidence: The Law and Science of Expert Testimony, Admissibility of scientific evidence: The general Acceptance Standard of Frye*, St. Paul, Minn.: West Publishing co., 2° ed., 2002, §§ 1, 2, pp. 4 ss., i quali, inoltre fanno notare come il *Frye test* altro non fosse che una versione del precedente *commercial marketplace test*, in cui viene cambiato il mercato di riferimento. Non più quello economico, bensì, quello scientifico.

all'interno dell'àmbito di ricerca cui esso apparteneva. In altri termini, i giudici statunitensi affermarono che la scientificità di una determinata tecnica dovesse essere desunta dall'affidabilità accademica del metodo prescelto. Se la comunità scientifica di riferimento avesse accettato, nella sua maggioranza, quello strumento come valido, allora quella tecnica avrebbe dovuto ritenersi scientifica e, quindi, utilizzabile nel processo[12]. Sulla scorta di questa sentenza nacque quello che è stato definito il c.d. *Frye test*.

Questo si fondava su una visione della scienza illimitata, completa e infallibile. Illimitata, in quanto alle leggi elaborate dalla scienza veniva riconosciuto un valore assoluto e generale; completa, perché il lavoro dello scienziato era ritenuto in grado di offrire una spiegazione integrale del fenomeno studiato; infallibile, perché il metodo scientifico era considerato immune da errori; eventuali risultato erronei erano da attribuire esclusivamente all'applicazione del metodo nel caso concreto[13]. Questa visione del fenomeno scientifico forma il presupposto culturale del *Frye test*. Infatti la possibilità che la comunità scientifica giunga ad un consenso stabile circa la validità di un certo strumento, presuppone una visione unitaria della scienza.

Dal punto di vista del rapporto tra processo e scienza, l'impostazione proposta dal *Frye test* poneva il giudice in una posizione passiva rispetto al fenomeno scientifico. La valutazione dell'organo giurisdizionale, infatti, era destinata ad appiattirsi su quella compiuta dalla comunità scientifica di riferimento. Se non vi era una generale accettazione del metodo, il giudice era costretto a dichiarare inammissibile la prova. Questa rigidità comportava, tra

[12] Si riporta il passaggio argomentativo centrale della sentenza: «*just when a scientific principle or discovery crosses the line between the experimental and demonstrable stages is difficult to define. Somewhere in this twilight zone the evidential force of the principle must be recognized, and while the courts will go a long way in admitting experimental testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs*» *Frye v. United States*, cit., 1014.

[13] Cfr. P. TONINI, *La prova scientifica: considerazioni introduttive*, in *La prova scientifica*, cit., p. 9.

l'altro, una certa chiusura del processo agli strumenti scientifici particolarmente innovativi e, di conseguenza, la sottrazione al giudice di utili elementi conoscitivi[14]. Soprattutto, il criterio della *general acceptance* non era in grado di evitare l'ingresso della c.d. *junk science* nel processo[15]. Infatti il *Frye test* lasciava impregiudicata la questione, fondamentale, circa la validità scientifica del metodo scelto. Il giudice non era chiamato a compiere una valutazione circa la scientificità della tecnica che si voleva utilizzare; ma doveva solo verificare se gli studiosi di quella branca della conoscenza umana ritenessero quello strumento come scientificamente valido[16].

Nonostante non avesse valore di precedente vincolante, il criterio della *general acceptance* divenne il punto di riferimento per la giurisprudenza nordamericana in tema di ammissione della prova scientifica.

Tuttavia, non mancarono pronunce che misero in discussione la validità del *Frye test*. Dal punto di vista cronologico una delle prime è *Coppolino v. State*[17]. Si trattava, come nel caso *Frye*, di un processo per omicidio. Questa volta la prova della quale si discuteva l'am-

[14] In tal senso, P.P. RIVELLO, *op. cit.*, pp. 77s. Per ulteriori spunti critici sul *Frye test*, v. O. DOMINIONI, *La prova penale*, cit., pp. 119 s. Da un diverso punto di vista, nella stessa dottrina nordamericana, è stato fatto notare come il *Frye test* potesse diventare uno *standard* fin troppo liberale. Infatti, la definizione di comunità scientifica di riferimento poteva influenzare la decisione del giudice circa la sussistenza o meno di un consenso: più ristretta fosse stata la comunità scientifica di riferimento, più semplice sarebbe stato trovare un consenso sulla validità di una certa tecnica. Cfr. DAVID L. FAIGMAN, DAVID H. KAYE, MICHAEL J. SAKS & JOSEPH SANDERS, *op. cit.*, pp. 9 s.

[15] Il termine è stato introdotto nel dibattito giuridico da P. HUBERT, *Galileo's Revenge: Junk Science in the Courtroom*, Basic books, New York, 1993, pp. 2 ss

[16] Icasticamente, M. TARUFFO, *Prova scientifica*, cit., pp. 969 s. fa notare come chiedere a coloro che praticano una certa professione se questa sia valida, possa portare a soluzioni tutt'altro che accettabili. Infatti, sicuramente un esperto di astrologia affermerebbe di essere in grado di offrire una effettiva conoscenza del futuro sulla base dell'analisi del moto dei pianeti.

[17] *Coppolino v. State*, 223 So.2d 68, 75 (Fla. Dist. Ct. App. 1969).

missibilità aveva per oggetto una tecnica finalizzata all'accertamento di condotte di avvelenamento[18]. La Corte, nel pronunciarsi sulla legittimità dell'ammissione dell'analisi tossicologica, rilevava come non fosse possibile per la società lasciare impunito un omicidio solo perché non si fosse formata una robusta letteratura scientifica su determinate sostanze[19]. I giudici rilevavano, in sostanza, l'inadeguatezza del *Frye test*, il quale non avrebbe mai permesso l'ingresso di tecniche nuove e avanzate all'interno del processo. Questo perché il raggiungimento di un consenso generalizzato su una certa tecnica non avrebbe mai potuto essere rapido. Nel momento in cui ci fosse stata una generale accettazione, la prova scientifica non si sarebbe più basata su strumenti all'avanguardia.

In questo panorama giurisprudenziale si inserì, nel 1975, la *Federal Rules of Evidence*, la quale regolò anche il fenomeno dell'assunzione dell'*expert testimony*. Più in particolare, tale tema è affrontato dalle *Rules* 702-706 *F.R.E.*, le quali, tuttavia, non fanno alcun riferimento al *Frye test*. Nasceva, quindi, la questione circa il valore da assegnare al *Frye test* nel nuovo contesto normativo. Sul tema si è sviluppata una giurisprudenza copiosa e frammentaria, il cui minimo comun denominatore è stato proprio il superamento del *Frye standard*[20]. Infatti anche quelle pronunce che ne accettavano la validità non lo applicavano in via esclusiva[21].

---

[18] Per una più ampia ricostruzione del fatto v. F. TAGLIARO – E. D'ALOJA – S. FREDERICK, *L'ammissibilità della «prova scientifica» in giudizio e il superamento del* Frye standard*: note sugli orientamenti negli USA successivi al caso* Daubert v. Merrell Dow Pharmaceuticals, inc., in *Riv. it. med. leg.*, 2000, pp. 721 s.

[19] «*The tests by which the medical examiner sought to determine whether death was caused by succinylcholine chloride were novel and devised specifically for this case. This does not render the evidence inadmissible. Society need not tolerate homicide until there develops a body of medical literature about some particular lethal agent. The expert witnesses were examined and cross-examined at great length and the jury could either believe or doubt the prosecution's testimony as it chose*» *Coppolino v. State*, cit., 75.

[20] Per una sommaria ricognizione degli orientamenti giurisprudenziali che mettevano in discussione il *Frye test*, v. O. DOMINIONI, *La prova penale*, cit., pp. 125 ss.

[21] Cfr. C. T. HUTCHINSON, D. S. ASHBY, *Daubert v. Merrell Dow Pharmaceuticals, Inc.: redefining the bases for admissibility of expert scientific testimony*, in *Cardozo L. Rev.*, 1994, p. 1882.

Quanto precisato, viene superato da un trittico di sentenze della Corte suprema degli Stati Uniti d'America[22]. La prima di queste pronunce ha origine da una causa intentata ad una casa farmaceutica da parte dei genitori di due ragazzi minori, affetti da gravi malformazioni. Ad avviso dei genitori, l'assunzione di un farmaco antinausea da parte della futura madre durante la gravidanza sarebbe stato alla base della successiva insorgenza delle suddette patologie. Si trattava di un *Bendectin case*: la correlazione tra questo farmaco antinausea e le malformazioni dei nascituri era già stata più volte portata all'attenzione della magistratura nordamericana. Tuttavia, i processi celebrati fino ad allora avevano avuto esiti molto diversi.[23].

Sullo sfondo della decisione si pone la già citata emanazione della *Federal Rules of Evidence*. Infatti la Corte suprema afferma di non poter fare altro che interpretare nella maniera più semplice e chiara possibile la *Rule* 702 *F.R.E.*, la quale si occupa dell'ammissibilità della *expert testimony*[24]. A parere dei giudici, in questa disposizione non è contenuto alcun riferimento al criterio della *general acceptance*. Non solo, il c.d. *Frye test* si pone in contrasto

[22] Si fa riferimento alla già citata *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, cit., nonché alle decisioni *General Electric Co. v. Joiner*, 522 U.S. 136 (1997), *Kumho Tire Company, Ltd. v. Carmichael*, 526 U.S. 137 (1999).

[23] In questo particolare processo, i genitori dei due minori fondavano la propria richiesta sulla base della testimonianza di otto esperti. Questi, oltre ad aver condotto degli studi in «vitro» e in «vivo», avevano analizzato la struttura chimica del farmaco, evidenziando le similarità tra il medicinale ed altre sostanze note per causare malformazioni alla nascita. Dall'altro lato, la casa farmaceutica si opponeva alle pretese dell'attore sulla base di un parere di un esperto ben qualificato. Egli fondava la propria opinione su di un'analisi della letteratura medica sul tema, la quale era formata da più di 30 pubblicazioni che avevano coinvolto circa 130.000 pazienti. Una parte delle argomentazioni poste a sostegno della casa farmaceutica fu pubblicata sul quotidiano *la Repubblica* dell'8 agosto 1993. Per una ricostruzione del fatto e del contesto storico della pronuncia, v. G. PONZANELLI, *Scienza, verità e diritto: il caso Bendectin*, in *Foro it.*, 1994, IV, cc. 184 s.

[24] La disposizione così afferma «*if scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise*». Tuttavia, alcuni Autori nordamericani fanno notare come l'interpretazione della *Rule* 702 non fosse uniforme nella giurisprudenza precedente al 1993, v. DAVID L. FAIGMAN, DAVID H. KAYE, MICHAEL J. SAKS & JOSEPH SANDERS, *op. cit.*, pp. 11 s. A sostegno di tale argomentazione, vengono citate le successive modifiche compiute sulla norma in discorso, al fine di rendere la stessa più in linea rispetto alla decisione della Corte suprema.

con l'impostazione di apertura al sapere scientifico contenuta nella *Federal Rules of Evidence*[25]. Per questo motivo, la regola della generale accettazione da parte della comunità scientifica di riferimento va rimeditata. Proseguendo nell'analisi della *Rule* 702 *F.R.E.*, la Corte suprema precisa come l'oggetto di tale *Rule* sia la testimonianza di un esperto, il quale deve farsi portatore di una conoscenza di carattere scientifico. Questa, per definirsi tale, deve trovare fondamento nel metodo scientifico.

Altro requisito che può essere fatto discendere dalla citata disposizione è quello dell'adeguatezza – concetto preso dalla precedente giurisprudenza e espresso dal termine «*fit*[26]» – del metodo scelto al fatto che deve essere accertato[27]. Quest'ultimo requisito è stato definito da alcuni eccessivamente fumoso e finalizzato a rafforzare l'utilità della prova in relazione ai fatti controversi[28]. Tuttavia, altri hanno rilevato come il concetto di adeguatezza sia facilmente definibile grazie ad un approccio casistico[29]. Proprio la pronuncia dalla quale si fa discendere tale nozione può essere utilizzata per definirlo. In *United States v. Downing* si discuteva della validità del riconoscimento dell'imputato compiuto da testimoni oculari. Più in particolare, venivano presentati studi per sostenere la fallibilità di una individuazione allorché il soggetto riconosciuto fosse di razza diversa rispetto a quello alla quale apparteneva la persona chiamata al riconoscimento oppure nel caso in cui quest'ultimo fosse sottoposto a forte stress. La Corte dichiarò inammissibile la prova in quanto mancava un nesso tra l'imputazione e l'oggetto della prova. Infatti nel processo in corso non si discuteva di identificazioni compiute su persone di razze diverse o da persone sottoposte a stress. In definitiva,

[25] Cfr. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, cit., 588, 589.

[26] Il termine risulta essere ripreso dalla sentenza *United States v. Dowing* 753 F.2d 1224, 1242 (Third Cir. 1985).

[27] Cfr. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, cit., 591.

[28] V. M. TARUFFO, *Le prove scientifiche*, cit., p. 237.

[29] Così, O. DOMINIONI, *La prova penale*, cit., p. 142.

dato che l'*expert testimony* deve essere utile al giudice del fatto per conoscere lo stesso, deve sussistere una connessione scientifica tra ciò che deve essere accertato e la testimonianza dell'esperto di cui si richiede l'ammissione.

Da quanto affermato, segue che due sono i presupposti per l'ammissione di una *expert testimony*. In primo luogo, il testimone deve essere portatore di una conoscenza scientifica; in secondo luogo, questi deve essere in grado di aiutare il giudice a comprendere correttamente il fatto oggetto di controversia[30]. Di conseguenza, diventa necessario per il giudice andare a controllare la validità del ragionamento o della metodologia su cui si basa la testimonianza dell'esperto e la loro adeguatezza ad essere utilizzati nel processo.

Ciò comporta l'ingresso nel dibattito giurisprudenziale dei temi, tutt'altro che scontati, della validità scientifica, della verificabilità empirica e della concezione di scienza. Tutti argomenti che nessun giudice può effettivamente padroneggiare propriamente. Come precisato nell'*opinion* di minoranza, il rischio è che il giudice si trasformi in uno scienziato dilettante[31].

Ad evitare un tale pericolo soccorre, secondo la Corte suprema, la c.d. «cultura di criteri[32]». Nella specie, la Corte suprema non si preoccupa di dare una definizione di scienza, o di metodo scientifico, piuttosto fornisce al giudice una serie di criteri finalizzati a distinguere

[30] Cfr. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, cit., 592, 593

[31] «*I do not doubt that Rule 702 confides to the judge some gatekeeping responsibility in deciding questions of the admissibility of proffered expert testimony. But I do not think it imposes on them either the obligation or the authority to become amateur scientists in order to perform that role*» *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, cit., 600.

[32] L'espressione è coniata da O. DOMINIONI, *La prova penale*, cit., pp. 69 ss. Secondo l'Autore, il giudice, attraverso la cultura di criteri, può uscire dal paradosso in cui si trova nel momento in cui deve valutare una prova scientifica. Questi, infatti, nomina un perito proprio perché riconosce la propria incapacità ad utilizzare determinate tecniche o metodologie. Tuttavia, la legge assegna al medesimo il compito di valutare le conclusioni cui è giunto il perito. Questo paradosso è superabile ammettendo la possibilità per il giudice di andare ad analizzare non le conclusioni dell'esperto, ma la validità e la correttezza del metodo da questi prescelto. Sul paradosso del giudice scienziato, cfr. M. TARUFFO, *La prova scientifica nel processo civile*, in *Riv. trim. dir. proc. civ.*, 2005, pp. 1109 ss.; C. CONTI, *op. cit.*, pp. 33 ss.

ciò che, con molta probabilità, è scienza da ciò che non lo è. Per compiere tale valutazione i giudici sono chiamati, innanzitutto, a controllare la verificabilità della teoria scientifica sottesa al parere dell'esperto. Inoltre, altra questione che deve essere affrontata in sede di ammissione della prova riguarda la sottoposizione della teoria o della tecnica al controllo dei membri della comunità scientifica attraverso la pubblicazione dei risultati delle ricerche su riviste specializzate. Questo criterio, precisano i giudici, non è da intendersi come decisivo, in quanto ben potrebbe accadere che della *junk science* sia introdotta in riviste prestigiose. Tuttavia, la pubblicazione dei risultati di una ricerca su un periodico specialista permette di evidenziare eventuali criticità della teoria o della tecnica che si vuole utilizzare. Non solo: il giudice deve, inoltre, conoscere il tasso di errore noto o potenziale rispetto agli *standards* richiesti dalla tecnica impiegata. Solo in ultima battuta, però, potrà farsi riferimento alla generale accettazione del metodo da parte della comunità scientifica di riferimento. Questo ultimo criterio deve essere visto come residuale e necessario solo a corroborare determinate ipotesi.

L'applicazione dei criteri enunciati non garantisce la certezza che la scienza spazzatura non sia introdotta nel processo. Tuttavia, sottolineano i giudici della Corte suprema, nel caso in cui si verifichi una tale eventualità, la possibilità che la decisione sia presa sulla base di un'errata comprensione del fatto è minimizzata da altri strumenti. Questi sono rappresentati sia dalla *cross examination* sia dall'ammissione di prove contrarie[33].

La griglia concettuale elaborata dalla Corte suprema deve essere utilizzata dal giudice in sede di ammissione della prova, affinché questi in quel momento svolga la funzione di guardiano – «*gatekeeper*» – della scientificità della prova[34].

[33] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, cit., 596.

[34] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, cit., 597.

La sentenza *Daubert* compie un nuovo e diverso bilanciamento tra scienza e processo. Infatti, in primo luogo, si manifesta un tentativo di permettere il più ampio uso possibile della scienza nel processo evitando, però, che vi faccia ingresso la c.d. *junk science*. In secondo luogo, tale sentenza merita di essere segnalata per il ruolo centrale che assegna al giudice: questi non è più obbligato ad affidarsi al parere di un esperto, in maniera passiva, ma acquista un ruolo attivo. Il giudice deve tenere conto del dibattito scientifico su di una determinata tecnica e sulla base di tale risultanze decidere se ammettere o meno una certa prova.

Successivamente alla citata sentenza *Daubert*, sono intervenute altre due pronunce della Corte suprema che sono andate a chiarire alcuni aspetti del c.d. *Daubert test*.

La prima di queste è stata emessa nel caso *General Electric Co. v. Joiner*[35]. Uno dei temi affrontato dalla pronuncia riguarda il c.d. *analytical gap*, espressione con la quale si fa riferimento al caso in cui non vi sia piena concordanza tra le premesse e le conclusioni dell'esperto di cui si chiede l'ammissione. In questa eventualità si pone il problema circa i limiti del potere del giudice in punto di ammissibilità della prova. I termini della questione riguardano la possibilità da parte dell'organo giurisdizionale di sindacare non solo la correttezza della metodologia scelta, ma anche la sua osservanza in relazione al caso concreto. I convenuti, infatti, sulla base di quanto sancito nella sentenza *Daubert*, affermavano che il giudice, in sede di ammissione della prova, dovesse focalizzare la propria attenzione solo sulla scientificità dei metodi scelti dall'esperto[36]. La Corte risponde a questa asserzione rilevando come il metodo e i risultati non possono essere considerati come elementi separati.

[35] *General Electric co. v. Joiner*, cit., per un'analisi più ampia della pronuncia e per gli opportuni riferimenti bibliografici anche in lingua inglese v. O. DOMINIONI, *La prova penale*, cit., pp. 179 – 186.

[36] L'affermazione, effettivamente presente in *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, cit., 595 aveva ingenerato un dibattito nella giurisprudenza e nella dottrina nordamericana; per una ricognizione del quale e per un inquadramento delle tematiche sottese alla distinzione tra metodologie e conclusioni, si rimanda a DAVID L. FAIGMAN, DAVID H. KAYE, MICHAEL J. SAKS & JOSEPH SANDERS, *op. cit.*, pp. 31 ss.

Infatti né quanto precisato nella sentenza *Daubert* né le F.R.E. autorizzano un giudice ad ammettere una prova scientifica nella quale si passi dalle premesse alle conclusioni solo sulla base di affermazioni non verificabili di un esperto[37]. Al contrario, il giudice è tenuto ad escludere la prova, tutte le volte in cui le inferenze che permettono di giungere a determinati risultati sulla base di determinati dati si rivelino inaffidabili. L'organo giurisdizionale è chiamato a compiere una valutazione unitaria che ha per oggetto tanto la metodologia quanto il risultato raggiunto[38]. Questa impostazione sicuramente rafforza il potere del giudice nella sua funzione di guardiano della scientificità della prova: questi, infatti, vede espandersi i suoi poteri di valutazione dell'ammissibilità della prova scientifica[39].

Il trittico di sentenze cui si è accennato si chiude con la decisione sul caso *Kumho Tire*[40], la quale, tra le altre cose, ha sancito la possibilità di applicare il c.d. *Daubert test* anche alle conoscenze di carattere tecnico. La Corte suprema nel decidere in tal senso va sia ad analizzare la lettera della *Rule* 702 delle F.R.E. sia la *ratio* della funzione di guardiano affidata al giudice.

In primo luogo, il testo della *Rule* 702 F.R.E. non autorizza alcuna distinzione tra tipologie di sapere. La disposizione, infatti, pone sullo stesso livello tanto le conoscenze scientifiche quanto quelle tecniche: entrambe possono essere oggetto di un'*expert testimony* purché questa raggiunga un sufficiente *standard* di affidabilità[41]. Le *Rule* 702, 703 F.R.E. prevedono

[37] Cfr. *General Electric co. v. Joiner*, cit., 146.

[38] In questo senso, v. S. LORUSSO, *La prova scientifica*, in *La prova penale*, diretto da A. Gaito, Utet, Torino, 2008, vol. I, p. 314.

[39] A parere di A. DONDI, *Problemi di utilizzazione delle «conoscenze esperte» come «*expert witness testimony*» nell'ordinamento statunitense*, in *Riv. trim. proc. civ.*, 2001, p. 1151, la centralità del ruolo del giudice ha come effetto anche quello di consentire allo stesso di individuare le migliori modalità di valutazione di conoscenze nuove.

[40] *Kumho Tire Company, Ltd v. Carmichael*, cit.

[41] Cfr. *Kumho Tire Company, Ltd v. Carmichael*, cit., 147.

una ampia libertà di ammissione dei consulenti tecnici in quanto questi abbiano una forte conoscenza della loro disciplina di riferimento. Questa facilità di ammissione non subisce alcuna limitazione sulla base della specie di conoscenze che l'esperto intende inserire nel processo.

In secondo luogo, sarebbe la stessa funzione di *gatekeeper* ad entrare in crisi laddove si introducesse una distinzione tra tipologie di sapere. Infatti la linea di demarcazione tra conoscenze tecniche e scientifiche è estremamente labile e sottile. In molti campi del sapere vi è uno stretto legame tra scienza e tecnica: molte discipline tecniche si fondano su leggi scientifiche. Alla luce di queste considerazioni, sarebbe pressoché impossibile per un giudice scegliere razionalmente quali prove ammettere e quali no[42].

Chiarita l'applicabilità generale del *Daubert test* a tutti i tipi di conoscenza, la Corte suprema riconosce al giudice la possibilità di modificare discrezionalmente i fattori da tenere in conto nella valutazione circa l'ammissibilità della prova in relazione all'oggetto della stessa. Infatti gli indici indicati nella sentenza *Daubert* non devono essere intesi come tassativi[43]. Questi devono adattarsi al caso concreto: può accadere che una determinata teoria non sia stata sottoposta alla *peer review* perché troppo innovativa; oppure che vi sia un generale

[42] Cfr. *Kumho Tire Company, Ltd v. Carmichael*, cit., 148.

[43] DAVID L. FAIGMAN, DAVID H. KAYE, MICHAEL J. SAKS & JOSEPH SANDERS, *op. cit.*, p. 42 fanno notare come l'eccessiva discrezionalità del giudice, se portata alle sue estreme conseguenze, potrebbe portare a risultati irrazionali. Infatti, ciascun giudice potrebbe scegliere per l'ammissione della medesima *expert testimony* dei criteri diversi per valutarne l'affidabilità. Nello stesso senso si esprime anche il giudice A. Scalia nella sua *concurring opinion*: «[…] *as the Court makes clear today, the Daubert factors are not holy writ, in a particular case the failure to apply one or another of them may be unreasonable, and hence an abuse of discretion*» *Kumho Tire Company, Ltd v. Carmichael*, cit., 159.

consenso tra gli esperti del settore, in una branca ampiamente riconosciuta come pseudo-scientifica[44]. Tuttavia, nessuno di questi fattori preso singolarmente può portare all'esclusione di una prova da parte del giudice[45].

[44] Cfr. *Kumho Tire Company, Ltd v. Carmichael*, cit., 151. Per ulteriori chiarimenti, v. O. DOMINIONI, *La prova penale*, cit., pp. 190 ss.

[45] Il capitolo conclusivo della vicenda esaminata è rappresentato dalla modifica della *Rule* 702 *F.R.E.*, la quale ora così dispone: «*a witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:*

(a) *the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;*

(b) *the testimony is based on sufficient facts or data;*

(c) *the testimony is the product of reliable principles and methods; and*

(d) *the expert has reliably applied the principles and methods to the facts of the case*». Per un breve commento alla modifica, v. O. DOMINIONI, *La prova penale*, cit., pp. 197 ss.

2. La prova scientifica nella normativa processuale penale italiana

Precisati sommariamente i termini del dibattito nordamericano sull'ammissione della prova scientifica, occorre riprendere il discorso interrotto. La prima questione da affrontare riguarda la definizione del termine prova scientifica. Infatti quella precedentemente individuata risulta essere relativamente imprecisa. L'indeterminatezza della perimetrazione effettuata affiora dall'analisi dell'art. 220 c.p.p., il quale si preoccupa di disciplinare l'oggetto della perizia. La norma impone al giudice di disporre una perizia tutte le volte in cui risulti necessario svolgere indagini, acquisire dati o valutazioni che richiedano specifiche competenze tecniche, scientifiche o artistiche[46]. Dalla lettura della disposizione emergono i tre compiti cui è chiamato il perito: rilevare dati impercettibili all'occhio del profano – compiere analisi nel caso di morte sospetta –; enunciare teoremi su premesse ipotetiche – quali siano i sintomi dell'avvelenamento da arsenico –; combinare rilievi sperimentali alle massime di esperienza al fine di elaborare conclusioni induttive – tizio è morto a causa dell'arsenico trovato nel suo corpo[47]. Alla luce del dato normativo, appare riduttivo ritenere che, per prova scientifica, si debba esclusivamente ritenere l'utilizzo, da parte del giudice, del sapere scientifico nel pas-

[46] La dottrina nella sua maggioranza riconosce in capo al giudice un obbligo di nomina del perito allorché sorga la necessità di utilizzare conoscenze specifiche in relazione ad un determinato tema di prova. Il riconoscimento di una situazione soggettiva di dovere si fonda sulla lettura della disposizione. Infatti, l'utilizzo dell'indicativo «è ammessa» riferito alla perizia, vale a circoscrivere la discrezionalità del giudice alla verifica del presupposto precisato dall'art. 220 c.p.p. Si riconosce, inoltre, il dovere del giudice di ammettere la perizia indipendentemente dalle eventuali conoscenze da lui possedute. Infatti, il perito risulta utile sia al giudice sia alle parti per poter stimolare il contraddittorio tra le stesse. Sul punto, v., fra i tanti, F. GIANFROTTA, *Art. 220*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. II, pp. 517 s.; più recentemente, C. VALENTINI, *I poteri del giudice dibattimentale nell'ammissione della prova*, Cedam, Padova, 2004, pp. 235 s. Dal canto suo, la giurisprudenza giunge a definire il potere del giudice come discrezionale, riconoscendo allo stesso un duplice spazio valutativo. L'organo giurisdizionale, infatti, è chiamato a valutare non solo l'esigenza circa l'accertamento di un determinato fatto, ma anche la possibilità di giungere a tale risultato attraverso altri mezzi di prova. Cfr. in motivazione, Cass. sez. V, 15 aprile 2004, Righetti ed altri, in *Arch. n. proc. pen.*, 2004, pp. 555 s.

[47] Cfr. F. CORDERO, *op. cit.*, pp. 781 s.

saggio dal fatto da provare al fatto provato. Questo, infatti, è solo uno degli aspetti caratterizzanti il fenomeno in discorso. In realtà, la dottrina più attenta ha rilevato come la nozione di prova scientifica nel processo penale sia più ampia. Questa, infatti, può essere definita come l'utilizzazione di strumenti tecnico scientifici all'interno di un determinato mezzo di prova[48].

Questa nozione, oltre a cogliere in maniera più precisa il fenomeno della prova scientifica, porta con sé un ulteriore vantaggio. Infatti implicita alla definizione riferita è l'idea per cui l'ingresso della scienza nel processo non avviene solo ed esclusivamente attraverso lo strumento della perizia. Astrattamente potrebbe sussistere una componente di carattere scientifico in ogni mezzo di prova[49].

La problematicità del tema della prova scientifica emerge già dalla definizione che è stata appena data. Infatti la prova scientifica appare come un contenitore vuoto, che viene riempito di volta in volta dalla tecnica che viene utilizzata nel caso concreto. Proprio sul materiale più adatto a riempire questo contenitore si focalizza gran parte del dibattito dottrinale. Infatti, il rapido progredire della scienza, unito al cambio di paradigma che si è registrato nella comunità scientifica hanno portato al centro del dibattito un nuovo elemento di

[48] La definizione è di O. DOMINIONI, *Prova scientifica*, cit., p. 977. L'Autore scompone i mezzi di prova tipici in cinque elementi. La fonte formale di prova, quella materiale, la specie di capacità conoscitiva, quella di elemento di prova e il nesso fra specie tipica di elemento di prova e le altre componenti tipiche funzionali all'ingresso di un mezzo di prova nel processo. Schematicamente, per fonte formale di prova, l'Autore intende quei meccanismi procedurali previsti dalla legge per l'introduzione nel processo, attraverso un mezzo di prova, di certi elementi conoscitivi. La fonte materiale di prova è costituita dalla persona o cosa che è in grado di apportare le conoscenze proprie del mezzo di prova. La specie di capacità conoscitiva è rappresentata dalla relazione in cui si trovano la fonte formale e la fonte materiale di prova. La specie di elemento di prova è ciò di cui il giudice si serve per la sua operazione inferenziale nella valutazione della prova. Infine, la legge tipizza il nesso funzionale che sussiste tra la specie di elemento di prova tipica e le componenti predisposte per l'ingresso di un mezzo di prova nel processo. In questa suddivisione, gli apparati conoscitivi propri della scienza risultano estranei alla tipizzazione legislativa. Questi, infatti, sono ricompresi in ciò che l'Autore definisce strumento di prova. V., *amplius*, O. DOMINIONI, *La prova penale*, cit., pp. 17 ss.

[49] Cfr. O. DOMINIONI, *La prova penale*, cit., p. 25.

discussione[50]. Ci riferisce alla c.d. prova scientifica nuova, ossia all'utilizzo nel processo penale di nuove ed avanzate tecniche scientifiche. Queste pongono gli studiosi del processo penale davanti a più complessi problemi, i quali riguardano tutte le fasi del procedimento probatorio. Infatti la tematica della prova scientifica nuova da un lato, ha riflessi importanti sull'ammissione, l'acquisizione e la valutazione della prova; dall'altro lato, si intreccia inevitabilmente con la tematica del contraddittorio su e per la formazione della prova[51].

Il tema dell'ammissione della prova è tra quelli che più contribuiscono a caratterizzare un sistema processuale. Due sono le principali problematiche connesse all'ammissione della prova e riguardano, rispettivamente, i soggetti legittimati a richiedere l'ammissione e i criteri in base ai quali ammettere una prova.

In ordine alla prima questione, il codice di rito vigente, in accordo con l'impostazione di stampo accusatorio accolta dalla legge delega, consegna principalmente alle parti il compito di chiedere l'ammissione delle prove[52]. Questa previsione si pone in linea con l'affermazione del principio del contraddittorio tra le parti[53]. Infatti la creazione di un effettivo scontro dialettico tra le parti riposa sul potere delle stesse di poter richiedere ed ottenere l'ammissione di prove a loro favore. È l'idea stessa che sta alla base del principio del contraddittorio

[50] Si fa riferimento al fenomeno denominato post-positivismo scientifico. Infatti, come chiarito da P. TONINI, *La prova scientifica*, cit., p. 9, si accetta ormai l'idea per cui la scienza sia limitata, incompleta e fallibile. Limitata, in quanto una legge scientifica è in grado di cogliere solo alcuni degli aspetti di un determinato fenomeno. Incompleta poiché ogni legge scientifica deve essere costantemente aggiornata oppure abbandonata sulla base delle nuove scoperte. Fallibile perché non esistono leggi scientifiche prive di un tasso di errore. Inoltre, si è registrato il passaggio dal c.d. verificazionismo al falsificazionismo. Una legge può dirsi scientifica solo se è sottoponibile a tentativi di falsificazione. Ciò comporta l'instabilità di qualsiasi conoscenza scientifica. Infatti, una legge scientifica può dirsi valida fino a quando non viene ritrovato anche un solo caso idoneo a smentirla. Per ulteriori riflessioni sul punto, v. P. FERRUA, *Metodo scientifico e processo penale*, in *La prova scientifica*, cit., pp. 12 ss.

[51] Cfr. G. CANZIO, *Prova scientifica, ricerca della "verità" e decisione giudiziaria nel processo penale*, in Aa. Vv., *Decisione giudiziaria e verità scientifica*, Giuffrè, Milano, 2005, pp. 57 s.

[52] Come eccezione al principio dispositivo, l'art. 190, co. 2° c.p.p. ammette la possibilità per la legge di prevedere casi di ammissione della prova da parte del giudice. Per un approfondimento circa i poteri ufficiosi del giudice in materia probatoria si rimanda, per tutti, a H. BELLUTA, *Imparzialità del giudice e dinamiche probatorie* ex officio, Giappichelli, Torino, 2006, pp. 55 ss.

[53] Cfr. P. TONINI, *Prova scientifica e contraddittorio*, in *Dir. pen. proc.*, 2003, p. 1459.

che impone un potere dispositivo delle parti in merito alle richieste di prova. Non solo, la disposizione dell'art. 190, co. 1° c.p.p. si pone come diretta applicazione degli artt. 24, 112 Cost. In relazione al primo, infatti, la disposizione codicistica dà concretezza al diritto di difesa, consentendo alle parti di «difendersi provando[54]». Per quanto attiene al secondo, l'obbligatorietà dell'azione penale non può che comportare anche la necessità di prevedere spazi per l'attività probatoria del pubblico ministero[55]. All'interno di queste coordinate si inserisce quello che è stato da alcuni definito il diritto alla prova scientifica. Infatti l'accettazione dell'idea post-positivista della scienza ha rilevanti ricadute sull'ammissione della prova scientifica. Ci si riferisce alle complessità emergenti dal pluralismo scientifico. Infatti come sottolineato dalla dottrina, è ben possibile che sussistano più tecniche o metodologie scientifiche idonee per l'accertamento di un determinato fatto. Questa considerazione comporta una molteplicità di ricadute sul tema dell'ammissione della prova. In primo luogo, l'eventualità che venga chiesta l'ammissione di più prove aventi per oggetto il medesimo fatto. In secondo luogo, poiché esistono più metodi di accertamento, il diritto alla prova di una parte non si limita solo all'ammissione degli strumenti idonei alla prova dei fatti a lei favorevoli, ma si estende anche al potere di richiedere l'ammissione di strumenti in grado di falsificare l'ipotesi della controparte[56]. In terzo luogo, data la possibilità che lo stesso elemento di prova

[54] Così, G. VASSALLI, *Il diritto alla prova nel processo penale*, in *Riv. it. dir. proc. pen.*, 1969, p. 12. L'Autore precisa, infatti, come la garanzia dell'inviolabilità della difesa non possa essere esclusivamente intesa come facoltà per le parti di essere rappresentate e di poter esporre le proprie ragioni davanti ad un giudice. L'art. 24 Cost. ha un valore più ampio, obbligando, inoltre, il legislatore a prevedere spazi per l'attività probatoria dell'imputato. In senso adesivo, v. Corte cost., 10 marzo 1994, n. 77, in *Giur. cost.*, 1994, pp. 776 ss.

[55] La dottrina riconosce l'operatività del principio di cui all'art. 112 Cost. anche oltre il momento finale di esercizio dell'azione penale. Da questa considerazione, discende l'obbligo di garantire alla pubblica accusa il diritto alla prova. Sui riflessi processuali del canone dell'obbligatorietà dell'azione penale v., V. GREVI, *Un'occasione perduta (o forse solo rinviata) dalla Corte costituzionale in tema di uso distorto della richiesta di rimessione del processo*, in *Cass. pen.*, 1996, p. 458; E. MARZADURI, *Azione, IV) diritto processuale penale*, in *Enc. giur. Treccani*, Roma, 1996, pp. 17 s.; G. UBERTIS, *Azione, II) azione penale*, in *Enc. giur. Treccani*, 1988, Roma, pp. 2 s.

[56] Così, P. TONINI, *Il diritto alla prova scientifica a dieci anni dalla sentenza Franzese*, in *Proc. pen. giust.*, 2012, n. 4, p. 3.

sia oggetto di diverse operazioni probatorie, ne segue che le parti, a meno che non si sia instaurato un contraddittorio tra di loro, non possono modificare in maniera irreversibile l'elemento di prova che è oggetto della prova scientifica[57].

Diverso è il discorso che deve essere affrontato per quanto attiene ai criteri che devono guidare il giudice nella scelta circa l'ammissione o meno di una prova. La questione è delicata, dal momento che, la valutazione sull'ammissibilità o meno del mezzo di prova deve essere condotta senza modificare il diritto alla prova delle parti. In quest'ottica, la dottrina distingue due diversi regimi di ammissibilità della prova: uno inclusivo e uno esclusivo[58].

Il primo è quello disciplinato dall'art. 190 c.p.p., il quale obbliga il giudice ad escludere le prove vietate dalla legge o manifestamente superflue o irrilevanti[59]. Dalla formulazione letterale della disposizione emerge come sulle parti non gravi alcun onere in merito alla dimostrazione circa la legittimità o la rilevanza della prova di cui si chiede l'ammissione. Pesa sull'autorità giurisdizionale il compito di rilevare la causa di inammissibilità e di dichiararla[60]. Ciò posto, la prima valutazione cui è chiamato il giudice è di carattere prettamente

[57] Ancora, P. TONINI, *Il diritto*, cit., p. 4.

[58] La distinzione accennata è di O. DOMINIONI, *L'ammissione della nuova prova penale scientifica*, in *La prova scientifica*, cit., p. 21.

[59] La disposizione si collega all'art. 111, co. 3° Cost. laddove prevede il diritto dell'imputato all'ammissione di «ogni mezzo [...] di prova a suo favore». Ad una prima lettura, questa disposizione sembrerebbe condurre ad escludere la validità dei criteri di cui all'art. 190 c.p.p. per le prove richieste dall'imputato. Infatti, la norma costituzionale parrebbe ammettere un indiscriminato diritto all'ammissione della prova per quest'ultimo. Tuttavia, la dottrina non ha mancato di sottolineare l'irragionevolezza dell'interpretazione riferita. Un tale sbilanciamento dei poteri di iniziativa probatoria suonerebbe discriminatorio per il pubblico ministero. Non solo, a conforto di un'interpretazione restrittiva dell'art. 111, co. 3° Cost. vi sarebbe anche un dato sistematico. Tra i canoni che vanno a definire il giusto processo, vi è anche quello della ragionevole durata. Sicuramente, l'indiscriminato potere di ammissione delle prove da parte dell'imputato finirebbe per frustare tale principio. V. sul punto, M. CHIAVARIO, *Art. 6*, in *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, a cura di S. Bartole – B. Conforti – G. Raimondi, Cedam, Padova, 2001, p. 239; F. CORDERO, *op. cit.*, p. 1298; E. MARZADURI, *Commento all'art. 1 l. cost. 23 novembre 1999, n. 2*, in *Leg. pen.*, 2000, p. 784.

[60] A. NAPPI, *Guida al codice di procedura penale*, Giuffrè, Milano, 10° ed., 2007, p. 125 fa rifermento ad una presunzione di ammissibilità delle prove richieste dalle parti. Nello stesso senso si è espressa Corte cost., 26 marzo 1993, n. 111, in *Giur. cost.*, 1993, pp. 901 ss.

giuridico: dichiarare l'inammissibilità di tutte le prove vietate dalla legge. Questo apprezzamento è logicamente precedente e assorbente rispetto a quello riguardante l'irrilevanza o la superfluità della prova. Infatti, una volta accertata l'illegittimità della prova, l'organo giurisdizionale non può fare altro che sancirne l'inammissibilità, non essendo previsto alcuno spazio nel processo per una prova rilevante ma inutilizzabile.

L'altro giudizio che deve essere compiuto ha carattere fattuale e ha per oggetto la manifesta non superfluità e la rilevanza della prova. Quest'ultimo concetto deve essere analizzato alla luce del disposto dell'art. 187 c.p.p., il quale definisce l'oggetto di prova. Dalla lettura combinata degli artt. 187 e 190 c.p.p. emerge quello che è stato da alcuni chiamato il criterio di rilevanza-pertinenza, il quale permette di definire rilevanti tutte le prove che risultino pertinenti all'oggetto della prova[61]. Ne deriva che la valutazione di irrilevanza della prova ha come suo punto di riferimento il fatto così come enunciato nell'imputazione, sulla base della perimetrazione effettuata in tale atto sarà possibile vagliare la rilevanza o meno di una determinata prova. Volendo scendere ancora più nello specifico, si può affermare come il controllo sulla rilevanza sia di carattere estrinseco, non potendo in alcun modo il giudice valutare, in sede ammissiva, la concludenza o meno della prova richiesta[62]. Discorso non troppo diverso deve essere condotto circa il concetto di superfluità. Anche questo è ricavabile per relazione: questa volta, però, il termine di riferimento è rappresentato dall'intero compendio probatorio richiesto dalla parte. Infatti la prova superflua è quella che tende a moltiplicare inutilmente le verifiche su di un certo tema di prova[63]. In altri termini, la prova superflua è

[61] In tal senso, V. GREVI, *Prove*, cit., p. 290.

[62] V., in giurisprudenza, Cass. sez. IV, 7 febbraio 1996, p.m. in c. Tollardo, in *C.e.d. cass.* n. 204589; Cass. sez. VI, 21 ottobre 2004, Cantanna ed altri, in *C.e.d. cass.* n. 231130.

[63] Cfr. M. NOBILI, *Art. 190*, in *Commento*, cit., p. 402; D. SIRACUSANO, *op. cit.*, p. 9.

quella che non è in grado di apportare alcun ulteriore elemento utile alla piattaforma probatoria di cui si servirà il giudice al termine dell'istruzione dibattimentale[64].

Il giudizio fattuale del giudice è ulteriormente limitato dall'avverbio «manifestamente». Infatti l'irrilevanza o la superfluità devono emergere *ictu oculi*, senza che sia necessaria alcuna particolare attività di approfondimento. In questo momento, come già precisato, il dubbio gioca a favore della parte richiedente: l'inammissibilità può derivare solo da un'irrilevanza o superfluità che si appalesi immediatamente agli occhi dell'autorità giurisdizionale[65]. In definitiva, il codice di rito penale consegna a quest'ultima un potere di filtro circa l'ammissione della prova estremamente limitato. Infatti, al fine di garantire la piena esplicazione del diritto alla prova, il legislatore ha escluso qualsiasi possibilità per il giudice di compiere, in sede di ammissione della prova, alcun giudizio sull'utilità o sul valore della stessa[66].

Il secondo regime di ammissione della prova è quello espresso nell'art. 189 c.p.p. La disposizione si occupa del controverso tema dell'ammissione delle prove atipiche[67]. Quest'ultima espressione, secondo la dottrina, può riferirsi a fenomeni diversi. In una prima acce-

[64] V., N. TRIGGIANI, *Il «diritto alla prova» nel nuovo codice di procedura penale*, in *Arch. n. proc. pen.*, 1991, p. 668.

[65] In tal senso, M. CHIAVARIO, *Considerazioni sul diritto alla prova nel processo penale*, in *Cass. pen.*, 1996, p. 2018; L. P. COMOGLIO, *Prove ed accertamento dei fatti nel nuovo c.p.p.*, in *Riv. it. dir. proc. pen.*, 1990, pp. 135 s.

[66] Cfr. O. DOMINIONI, *L'ammissione*, cit., p. 21.

[67] Durante la vigenza del codice del 1930, la dottrina e la giurisprudenza discussero della opportunità di prevedere l'ammissibilità di prove atipiche. Tra le voci favorevoli alla tassatività dei mezzi di prova, spiccano, per autorevolezza, quelle di G. CONSO, *Natura giuridica delle norme sulla prova nel processo penale*, in *Riv. dir. proc.*, 1970, pp. 19 s. e di G. LEONE, *Svolgimento del processo penale. Il processo di prima istanza*, in G. Leone, *Trattato di diritto processuale penale*, Jovene, Napoli, 1961, vol. I, pp. 175 ss. Entrambi gli Autori ritengono che l'inviolabilità del diritto di difesa comporti l'inammissibilità di prove non consentite dalla legge. In questa scia si inserisce il progetto del codice di procedura penale del 1978, il quale prese una posizione molto netta sul punto. Infatti, l'art. 179 stabiliva che «il giudice non può ammettere prove diverse da quelle previste dalla legge». La motivazione alla base di tale scelta era duplice. In primo luogo, evitare qualsiasi possibilità di abuso nell'utilizzo di strumenti non idonei all'accertamento del fatto. In secondo luogo, bilanciare l'esigenza di accertamento del fatto con altri valori di pari livello, quali il diritto di difesa delle parti e la soggezione del giudice soltanto alla legge. Cfr. E. ZAPPALÀ, *Il principio di tassatività dei mezzi di prova nel processo penale*, Giuffrè, Milano, 1982, pp. 91 s.

zione, essa allude «alla fonte del convincimento del giudice», ossia dell'esistenza di uno strumento gnoseologico sconosciuto dalla realtà processuale[68]. Ma l'atipicità può riferirsi anche al «modo in cui il mezzo di prova si è costituito»[69]. L'atipicità, in questo secondo caso, ha per oggetto l'attività di creazione del mezzo di prova, la quale viene compiuta in maniera divergente rispetto a quanto previsto dalla legge. Ne è un esempio, quello della c.d. ricognizione informale, ossia del caso in cui la persona offesa riconosca in dibattimento l'imputato senza che tale attività sia eseguita rispettando le forme di cui agli artt. 213, 214 c.p.p. Di queste due accezioni solo nel primo caso avremmo una prova atipica in senso proprio. Nel secondo, invece, si delineerebbe il fenomeno delle prove assunte *contra legem*[70]. L'argomentazione che porta a tale conclusione ha come punto di partenza la corretta comprensione dei concetti di tipicità e di tassatività della prova. Infatti il legislatore, oltre a creare un catalogo di prove tipiche, ha, inoltre, compiuto una scelta di tassatività in relazione alla formazione del risultato di prova[71]. In altri termini, all'interno del codice di procedura penale la scelta compiuta è stata, da un lato, quella di regolare le forme attraverso le quali determinate conoscenze possono entrare nel processo e, dall'altro, di sanzionare con l'inutilizzabilità il mancato ri-

[68] Così, R. ORLANDI, *Atti e informazioni dell'autorità amministrativa nel processo penale. Contributo allo studio delle prove extrapenali*, Giuffrè, Milano, 1992, p. 24.

[69] Ancora, R. ORLANDI, *op. cit.*, p. 24.

[70] Cfr., M. NOBILI, *Art. 189*, in *Commento*, cit., p. 398.

[71] Dal canto suo, la giurisprudenza tende ad espandere i poteri istruttori del giudice riconoscendogli una sorta di libertà della prova. Ciò sulla base di una particolare interpretazione del principio del libero convincimento del giudice e della non tassatività dei mezzi di prova. Infatti, entrambi questi canoni permetterebbero all'autorità giurisdizionale di utilizzare per la formazione del proprio convincimento tutti gli elementi probatori disponibili. Tra le più recenti sul punto, v. Cass. sez. V, 19 febbraio 2014, De Benedetto, in *C.e.d. cass.* n. 263168. La dottrina non ha mancato di stigmatizzare una tale impostazione, rilevando come i princìpi richiamati non si pongano in opposizione all'atipicità probatoria. Infatti, il libero convincimento del giudice opera in sede di valutazione della prova e presuppone l'assunzione della stessa nel rispetto della legge. Inoltre, la non tassatività dei mezzi di prova non può condurre all'utilizzazione di prove assunte in violazione delle norme di formazione delle stesse. In relazione al codice del 1930 v. E. ZAPPALÀ, *op. cit.*, pp. 112 s.; in riferimento all'attuale codice di rito, tra i tanti, v. G.F. RICCI, *Le prove atipiche*, Giuffrè, Milano, 1999, p. 529.

spetto di queste forme. Sul punto la dottrina giunge ad individuare un principio di infungibilità tra metodi probatori[72]. All'interno di tale corrente dottrinale, non manca chi accolga una impostazione meno rigida[73]. Infatti sarebbe opportuno distinguere i casi in cui il legislatore agganci alla tipicità di un mezzo di prova anche la tassatività, dai casi in cui questa unione non si verifica. Secondo questa impostazione, sarebbe da considerare come prova atipica valida, anche quella che si forma in maniera diversa rispetto al modello legale, senza, però, dare luogo a qualche forma di invalidità[74].

Definito sommariamente il campo di applicazione dell'art. 189 c.p.p., è necessario ora passare ad esaminare il criterio di ammissione della prova atipica. Come già anticipato, il vaglio di ammissibilità dettato per la prova atipica è, da alcuni, definito di tipo esclusivo[75]. Infatti per l'ammissione di una prova atipica è necessaria la sussistenza di due elementi di carattere qualificante: l'idoneità all'accertamento del fatto e la non lesività della libertà morale della persona[76]. Il primo, giustificato alla luce della presunzione di idoneità all'accertamento del fatto che sorregge soltanto i mezzi di prova tipici[77], è da intendersi come capacità astratta del mezzo di prova richiesto di fornire al giudice una ricostruzione attendibile del fatto[78]. Il secondo costituisce una riaffermazione del principio generale in materia probatoria espresso dall'art. 188 c.p.p.

---

[72] In tal senso, M. NOBILI, *Art. 189*, cit., p. 398. La medesima prospettiva è accolta, tra gli altri, anche da C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, Padova, 2007, pp. 274 ss.; T. RAFARACI, *Ricognizione informale dell'imputato e (pretesa) fungibilità delle forme probatorie*, in *Cass. pen.*, 1998, p. 1741.

[73] Ci si riferisce a quanto scritto da O. DOMINIONI, *La prova penale*, cit., pp. 89 ss.

[74] Cfr. O. DOMINIONI, *La prova penale*, cit., p. 90.

[75] V., O. DOMINIONI, *L'ammissione*, cit., p. 21.

[76] La dottrina ha precisato come la sussistenza di questi due requisiti sia il primo gradino che deve essere superato dalla prova atipica per entrare nel processo penale. Infatti, anche le prove atipiche sono sottoposte allo scrutinio di cui all'art. 190 c.p.p. V., sul punto, V. GREVI, *Prove*, cit., p. 292.

[77] Tra i tanti, v. D. SIRACUSANO, *op. cit.*, p. 4.

[78] La dottrina sottolinea l'importanza di una valutazione astratta, al fine di evitare la confusione tra il giudizio di cui all'art. 189 c.p.p. e quello dell'art. 190 c.p.p. Infatti, ad evitare che vengano introdotti nel processo penale strumenti conoscitivi che non possano fornire al giudice degli elementi utili per fondare il proprio convincimento, il

Chiariti sommariamente i regimi di ammissione della prova nel processo penale, deve essere sottolineato come si registri in dottrina un dibattito circa gli strumenti da utilizzare in sede di ammissione di una prova scientifica nuova. Secondo alcuni l'ammissione della prova scientifica nuova dovrebbe essere disposta in base all'art. 189 c.p.p.[79]; secondo altri, occorrerebbe fare riferimento a quanto stabilito dall'art. 190 c.p.p.[80]; per altri ancora la regola di ammissione della prova scientifica nuova sarebbe contenuta nell'art. 220 c.p.p.[81].

La prima impostazione è sostenuta da un duplice livello di argomentazioni: uno storico e logico sistematico, l'altro analogico. In prima battuta, è necessario superare l'interpretazione letterale dell'art. 189 c.p.p. Infatti l'espressione «prove non disciplinate dalla legge» sembrerebbe condurre all'applicazione della disposizione in commento soltanto alle prove atipiche in senso proprio. Tuttavia, rilevanti fattori tanto logico-sistematici quanto storici conducono a svalutare l'importanza della lettera della norma. Infatti la prospettiva di carattere storico evidenzia come l'art. 189 c.p.p. sia stato inserito nel testo del codice di rito penale proprio per permettere l'ingresso nel processo penale di nuove e avanzate tecniche di indagine[82]. Questa considerazione fa emergere come la *ratio* sottesa all'art. 189 c.p.p. sia proprio quella dell'apertura del processo alla scienza più innovativa[83]. Non solo, l'art. 189 c.p.p. non

codice di rito penale prevede il potere del giudice di non ammettere le prove considerate irrilevanti. Per ulteriori considerazioni sul punto si rimanda a G.F. RICCI, *op. cit.*, p. 537.

[79] La prima impostazione, sostenuta in principio da O. DOMINIONI, *La prova penale*, cit., pp. 102 ss., è stata successivamente fatta propria da F. CASASOLE, *Neuroscienze, genetica comportamentale e processo penale*, in *Dir. pen. proc.*, 2012, pp. 113 s.; I. PALMA, *Considerazioni sul principio di tassatività dei mezzi di prova*, in *Riv. it. dir. proc. pen.*, 2009, p. 413.

[80] F. CAPRIOLI, *op. cit.*, p. 1872; P. FELICIONI, *Prova scientifica*, in *Dig. pen.*, Utet, Torino, 2014, agg. VIII, p. 624; S. LORUSSO, *op. cit.*, pp. 322 ss.; G. UBERTIS, *La prova scientifica e la nottola di Minerva*, in *La prova scientifica nel processo penale*, a cura di L. De Cataldo Neuburger, Cedam, Padova, 2007, pp. 83 ss.

[81] F. FOCARDI, *La consulenza tecnica extraperitale delle parti private*, Cedam, Padova, 2003, pp. 190 ss.

[82] La *Rel. prog. prel.*, in *Speciale documenti giustizia*, II, 1988, p. 60 in relazione all'art. 189 c.p.p. precisava che «è sembrato che una norma così articolata possa evitare successive 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».

[83] Cfr. O. DOMINIONI, *La prova penale*, cit., p. 103.

sarebbe la norma che legittimerebbe l'atipicità probatoria nel sistema, esso conterrebbe esclusivamente le norme per il suo impiego[84]. Per cui, la riconduzione della prova scientifica nuova alla disposizione citata non avrebbe nessuna influenza sull'estensione del catalogo delle prove disciplinate dal legislatore. Si tratterebbe, più semplicemente, di applicare alla prova scientifica nuova le speciali norme di assunzione previste per la prova atipica[85]. Inoltre, la prova scientifica nuova presenterebbe una fenomenologia molto simile a quella descritta dall'art. 189 c.p.p.[86]. Queste ragioni dovrebbero condurre l'interprete a ritenere la sussistenza sia delle prove atipiche in senso proprio, ossia di quelle prove che sono assenti nel catalogo legale, sia di quelle atipiche in senso improprio, ovvero della prova scientifica nuova.

Sempre a parere della medesima dottrina, esisterebbe un altro percorso argomentativo per arrivare a sostenere l'applicazione dell'art. 189 c.p.p. alla prova scientifica nuova. Questa si poggia sull'analogia tra le problematiche che ordinariamente pone una prova atipica e quelle che afferiscono alla prova scientifica nuova. In questa prospettiva va sottolineato anzitutto come, tutte le volte in cui debba essere ammessa una prova atipica, nasca la necessità di sondarne l'idoneità all'accertamento del fatto e di evitare che questa possa essere lesiva della libertà morale del soggetto che vi è sottoposto[87]. Solo i mezzi di prova tipici, infatti, sono presunti idonei e rispettosi dei diritti della persona dal legislatore. La medesima

[84] In tal senso, ancora, O. DOMINIONI, *La prova penale*, cit., p. 88.

[85] V., O. DOMINIONI, *La prova penale*, cit., p. 103.

[86] Cfr. C. BRUSCO, *Il vizio di motivazione nella valutazione della prova scientifica*, in *Dir. pen. proc.*, 2004, p. 1415; O. DOMINIONI, *La prova penale*, cit., p. 103. In senso parzialmente conforme, v. P. MOSCARINI, *Lo statuto della "prova scientifica" nel processo penale*, in *Dir. pen. proc*, 2015, p. 656, il quale, pur riconoscendo l'analogia sussistente tra le prove atipiche e le prove scientifiche nuove critica l'applicazione dell'art. 189 c.p.p. al fenomeno della *novel science*.

[87] Sul punto, v. *supra* nt. 80.

problematica risulta sussistente anche per la prova scientifica nuova, la quale, in quanto sconosciuta all'àmbito giudiziario o assistita da risultati controversi, pone rilevanti problemi in tema di capacità di accertamento del fatto e di tutela dei diritti del singolo[88]. Inoltre, sia sul fronte della prova atipica, sia su quello della prova scientifica, ragioni di economia processuale impongono che la valutazione cui si è accennato venga compiuta all'inizio del processo. Motivazioni simili impongono uno scrutinio circa la validità scientifica della metodologia prescelta al fine di evitare inutili e dispendiose attività processuali. In terzo luogo, l'art. 189 c.p.p. prescrive che le modalità di assunzione della prova siano individuate dal giudice sulla base di quanto richiesto dalle parti. Ciò in quanto, trattandosi di prove non disciplinate dalla legge si impone la necessità di disporre metodi acquisitivi specifici. Simmetricamente, l'assunzione di prove che utilizzano strumenti nuovi o controversi può comportare la necessità di ridefinire le modalità di acquisizione degli stessi. Quanto rilevato fa emergere la chiara analogia sussistente tra il fenomeno dell'atipicità probatoria e quello della prova scientifica nuova[89].

Il pregio più rilevante di questa impostazione è rappresentato dalla funzione che assumerebbe il giudice in ordine all'ammissione della prova scientifica nuova. Questi, infatti, potrebbe svolgere appieno quella *gatekeeping function* di cui si è accennato nel paragrafo precedente. Sarebbe il concetto stesso di idoneità all'accertamento del fatto a condurre ad una tale soluzione. All'interno di tale parametro, l'organo giurisdizionale sarebbe chiamato a valutare tutte le questioni attinenti alla validità teorica del principio scientifico utilizzato nel mezzo di prova richiesto[90].

[88] Così si esprime O. DOMINIONI, *La prova penale*, cit., pp. 104 s.

[89] F. CASASOLE, *op. cit.*, p. 114; O. DOMINIONI, *La prova penale*, cit., pp. 210 ss.

[90] Questa impostazione viene già accennata in O. DOMINIONI, *In tema di nuova prova scientifica*, in *Dir. pen. proc.*, 2001, p. 1063 e sostenuta anche da G. CANZIO, *Prova scientifica, ragionamento probatorio e libero convincimento del*

La tesi appena esposta è stata oggetto di critica da parte di altra dottrina che ha sollevato, al riguardo, diverse obiezioni. In primo luogo, viene posta in discussione l'applicazione in maniera analogica dell'art. 189 c.p.p.[91]. A parere di questa dottrina, infatti, esisterebbe un principio di legalità processuale che impedirebbe l'applicazione analogica delle norme processuali. Tale canone troverebbe la sua fonte sia nell'art. 111, co. 1° Cost. sia nei princìpi generali di diritto riconosciuti dalla Corte europea dei diritti dell'uomo[92]. In secondo luogo, viene sottolineato come l'orientamento criticato lederebbe l'imparzialità e la terzietà del giudice sotto il profilo della sua neutralità metodologica, imponendo allo stesso un giudizio di prevalutazione dell'attendibilità della prova[93]. In terzo luogo, si lamenta l'evidente forzatura del disposto di cui all'art. 189 c.p.p. Infatti l'applicazione della citata disposizione alle sole tecniche controverse introdurrebbe una distinzione arbitraria che non trova alcun riscontro nel testo della norma[94].

Scartata l'applicazione analogica dell'art. 189 c.p.p., questo filone dottrinario propone di ricondurre le tematiche del vaglio di ammissibilità delle prove scientifiche all'ultimo delle coordinate generali dettate dall'art. 190 c.p.p. Il perno del ragionamento sarebbe rappresentato dal concetto di «irrilevanza probatoria per inidoneità[95]».

---

giudice nel processo penale, in *Dir. pen. proc.*, 2003, pp. 1194 s. V. più diffusamente, O. DOMINIONI, *La prova penale*, cit., pp. 210 ss.

[91] Così, G. UBERTIS, *Il giudice, la scienza e la prova*, in *Cass. pen.*, 2011, p. 4113.

[92] V. Corte eur,. 22 giugno 2000, Coëme e altri c. Belgio, § 102. G. UBERTIS, *Il giudice*, cit., p. 4113, inoltre, pone in dubbio il collegamento che sussisterebbe tra gli artt. 189, 190 c.p.p. Infatti, i due criteri contenuti nelle disposizioni citate non si porrebbero tra loro in un rapporto di regola ed eccezione, ma, più correttamente, costituirebbero una regolamentazione unitaria della materia. In senso adesivo all'opinione riportata, v. P. FELICIONI, *op. cit.*, p. 624.

[93] Cfr., P.P. RIVELLO, *op. cit.*, p. 130, il quale, inoltre, paventa il pericolo di una chiusura del processo alla scienza. Infatti, il giudice davanti alla prova scientifica controversa potrebbe essere indotto ad applicare in maniera rigorosa l'art. 189 c.p.p. adottando un provvedimento di esclusione della prova.

[94] In questi termini si esprime, F. CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, p. 3529, il quale, inoltre, fa notare la difficoltà di avere una definizione sufficientemente precisa di *novel science*.

[95] L'espressione è di G. UBERTIS, *La prova scientifica*, cit., p. 87. L'Autore ritiene di aver ritrovato una nozione affine alla rilevanza idoneità nei concetti di «rilevanza in fatto» e «rilevanza in senso stretto» studiati rispettivamente da D. SIRACUSANO, *Studio sulla prova delle esimenti*, Giuffrè, Milano, 1959, p. 58; M. TARUFFO, *Studi sulla rilevanza*

Punto di partenza è il capovolgimento del tradizionale rapporto tra ammissione e valutazione della prova. È ben vero che il potere di valutazione della prova del giudice si esercita solo sugli elementi probatori ammessi. Tuttavia, deve essere sottolineato come la futura valutazione della prova incida sul giudizio di ammissione di un certo mezzo di prova[96]. Secondo questa impostazione, sarebbe insensato ammettere ciò che non potrebbe, successivamente, essere valutato. All'interno di questa cornice si inserirebbe la valutazione di rilevanza-idoneità del mezzo di prova. Questa va intesa come la capacità del mezzo di prova di apportare elementi utili da cui inferire proposizioni che siano in grado di confermare o smentire l'affermazione probatoria integrante l'oggetto di prova. Esemplificando, dovrebbe essere dichiarata inammissibile la testimonianza di un testimone daltonico, la cui malattia sia pacificamente accettata dalle parti, nel caso in cui l'oggetto della prova sia il colore della macchina usata per una rapina[97]. Sempre sulla base del rapporto esistente tra ammissione e valutazione probatoria, deve essere rilevata l'inidoneità probatoria di quei mezzi di prova che, basandosi su leggi scientifiche prive di opportuni riscontri, non possano essere utilizzate dal giudice per decidere in relazione al *thema probandum*[98]. Si sottolinea, infine, come il giudice che compia una tale valutazione mantenga la propria neutralità metodologica. Infatti l'organo giurisdizionale è chiamato, secondo tale impostazione, a compiere esclusivamente un giudizio sulla capacità della tecnica che si intende impiegare di poter giungere ad un risultato fruibile in relazione a ciò che deve essere provato[99].

---

della prova, Cedam, Padova, 1970, p. 33. Per una critica a questa ricostruzione, v. O. DOMINIONI, *La prova penale*, cit., p. 222.

[96] Ancora G. UBERTIS, *La prova scientifica*, cit., p. 87. V., inoltre, S. LORUSSO, *op. cit.*, p. 323; P. FELICIONI, *op. cit.*, p. 624.

[97] L'esempio è proposto da G. UBERTIS, *La prova scientifica*, cit., p. 88.

[98] Ammettono una tale impostazione anche F. CAPRIOLI, *La scienza*, cit., p. 3529; S. LORUSSO, *op. cit.*, p. 323.

[99] Cfr. G. UBERTIS, *La prova scientifica*, cit., p. 90; P.P. RIVELLO, *op. cit.*, p. 132.

Anche questo orientamento è stato sottoposto a critica, sottolineando, in particolare, l'eccessivo potere consegnato al giudice in fase di ammissione della prova. Infatti l'idoneità cui fa riferimento la dottrina contestata riguarderebbe la capacità concreta della fonte di prova o del mezzo di prova di poter fornire elementi utili al giudice[100]. Tuttavia, tale giudizio non può essere compiuto in fase di ammissione della prova, senza che vi sia una prevalutazione della stessa[101]. Inoltre, si è da altri sottolineato come, l'art. 190 c.p.p. non sembrerebbe essere lo strumento migliore per evitare l'ingresso della scienza spazzatura nel processo. Infatti la prova scientifica basata su un metodo errato non può essere considerata né *contra legem*, né superflua – in quanto le parti potrebbero non aver presentato altri mezzi di prova in relazione a quel fatto – e nemmeno irrilevante – poiché la rilevanza riguarda l'oggetto di prova e non il metodo con cui si vorrebbe giungere ad un certo risultato probatorio[102].

Esiste una terza e, per la verità, minoritaria opinione sugli strumenti normativi più adatti a regolare l'ingresso della *novel science* nel processo[103]. Punto di partenza di questa tesi è l'importanza del principio *iura novit curia,* sulla base del quale compete al giudice qualificare giuridicamente lo strumento di cui si chiede l'ammissione come prova, individuando se questo sia un mezzo di prova tipica e, in caso di risposta affermativa, quale. Nel momento in cui una parte richiede l'ammissione di una consulenza tecnica o una perizia, l'autorità giurisdizionale avrebbe il potere di escludere tale mezzo di prova tutte le volte in cui questo si basi su metodologie scientifiche errate. Infatti una consulenza tecnica che utilizzi sapere non

[100] G. UBERTIS, *La prova penale. Profili giuridici ed epistemologici*, Utet, Torino, 1995, p. 27, definisce fonte di prova il soggetto o l'oggetto da cui può derivare un elemento di prova e mezzo di prova l'attività attraverso cui viene introdotto nel procedimento un elemento di prova.

[101] Cfr. O. DOMINIONI, *La prova penale*, cit., p. 222, nt. 32.

[102] Così si esprime F. FOCARDI, *op. cit.*, p. 190.

[103] Ci si riferisce a quanto affermato da F. FOCARDI, *op. cit.*, pp. 191 ss.

scientifico non potrebbe essere considerata tale[104]. Nella valutazione sulla scientificità della tecnica che si intende impiegare il giudice potrebbe, secondo questo indirizzo, impiegare i criteri elaborati dalla giurisprudenza nordamericana.

La principale obiezione che viene mossa a tale impostazione ha per oggetto la corretta ricostruzione delle componenti dei mezzi di prova. L'art. 220, co. 1° c.p.p. ammette la possibilità per il giudice di valutare esclusivamente la capacità conoscitiva del perito, il quale deve possedere specifiche conoscenze tecniche, scientifiche o artistiche. Tuttavia, ciò che dovrebbe essere oggetto di attento scrutinio da parte del giudice allorché si voglia introdurre nel processo la *novel science* è la validità scientifica dello strumento richiesto[105].

Del dibattito appena esposto si trova un breve accenno in una sentenza riguardante un famoso caso di cronaca[106]. Ci si riferisce all'omicidio di Samuele Lorenzi avvenuto a Cogne il 30 gennaio 2002, per il quale la madre dello stesso è stata condannata alla pena di sedici anni di reclusione. Tra le numerose e complesse fonti del convincimento del giudice vi erano anche i risultati di una perizia svolta in incidente probatorio, la quale ha utilizzato una innovativa tecnica scientifica che, dalla consistenza e tipologia delle macchie di sangue, era in grado di inferire le modalità di svolgimento dell'attività criminosa. Tale metodologia è definita *Bloodstain Pattern Analysis*[107].

---

[104] Cfr. F. FOCARDI, *op. cit.*, p. 192. L'Autore cita a sostegno della propria tesi Trib. Palermo, ord. 21 maggio 1996, Andreotti, in *Dir. pen. proc.*, 1997, p. 333. In quel provvedimento veniva esclusa l'ammissione di una consulenza tecnica avente per oggetto la ricostruzione dell'origine e dell'evoluzione della corrente andreottiana all'interno della Democrazia Cristiana. La motivazione dell'ordinanza offriva una rilettura in negativo dell'art. 233 c.p.p., rilevando come non fosse possibile ammettere una consulenza tecnica allorché l'esperto chiamato non avesse applicato leggi scientifiche.

[105] In tal senso, O. DOMINIONI, *La prova penale*, cit., p. 107.

[106] Cfr. Cass. sez. I, 21 maggio 2008, Franzoni, in *C.e.d. cass.* n. 240764.

[107] Per un inquadramento generale della *BPA* si rimanda a S. CAPITANI, *Brevi considerazioni sulla* Bloodstain pattern analysis *nel procedimento penale*, in *Dir. pen. proc.*, 2015, pp. 487 ss.

Proprio l'impiego di tale strumento per l'accertamento del fatto di reato è stato oggetto di discussione tra le parti. Infatti la difesa dell'imputata, riecheggiando le argomentazioni della dottrina sopracitata, ritiene necessario qualificare la *BPA* come prova atipica. Sul punto, tuttavia, la risposta data dai giudici di legittimità è negativa. Infatti la particolarità dell'indagine richiesta non può comportare ad escludere l'applicazione al caso di specie della disposizione di cui all'art. 220 c.p.p. Questa norma, non tipizzando l'oggetto della perizia, permette un'applicazione estremamente flessibile del mezzo di prova in discorso[108]. L'argomentazione della Cassazione è stata ritenuta dalla dottrina corretta; tuttavia, è stato sottolineato come così facendo sia stata evitata la questione circa l'applicazione in via analogica dell'art. 189 c.p.p.[109].

[108] Cfr. Cass. sez. I, 21 maggio 2008, Franzoni, cit., p. 42.

[109] In tal senso, F. CAPRIOLI, Scientific evidence, cit., p. 1872. Deve essere segnalato, tuttavia, come l'Autore non sia tra i sostenitori dell'applicabilità dell'art. 189 c.p.p. alle prove scientifiche nuove.

3. La valutazione della prova scientifica

Sempre in relazione al tema della prova scientifica nuova, deve essere rilevato come la giurisprudenza, salve poche eccezioni abbia concentrato maggiormente la propria attenzione sul momento della valutazione rispetto a quello dell'ammissione della prova stessa.

Con l'espressione «valutazione della prova», si fa riferimento alla fase conclusiva del procedimento probatorio. In questo stadio, l'elemento di prova, ossia ciò che viene introdotto nel processo dalle parti, si trasforma in risultato probatorio attraverso una regola di inferenza. Tutto il tema ruota attorno al costante problema di garantire piena libertà di valutazione al giudice, evitando però che questo potere si trasformi in arbitrio. Per questo motivo, il legislatore ha deciso di indicare i parametri che devono guidare l'attività valutativa del giudice[110]. Questi sono precisati dall'art. 192 c.p.p., pietra angolare della valutazione della prova. Dalla lettura della disposizione, emerge la volontà da parte del codice di rito vigente di far propri all'interno del nostro sistema processuale il principio del libero convincimento del giudice[111]. Il significato minimo da attribuire ad una tale formula risiede nell'esclusione dal processo penale di qualsiasi criterio di prova legale[112]. In altri termini, tale canone impone di lasciare al giudice la possibilità di apprezzare liberamente il valore da assegnare alla

[110] G. DE LUCA, *Il sistema delle prove penali e il principio del libero convincimento nel nuovo rito*, in *Riv. it. dir. proc. pen.*, 1992, p. 1259, non manca di sottolineare come l'attività di giudizio sarebbe in astratto non sottoponibile ad alcuna regola.

[111] La scelta si pone in linea con l'abrogato codice di procedura penale; per alcuni brevi cenni storici, v. M. NOBILI, *Libero convincimento del giudice*, in *Enc. giur. Treccani*, Roma, 1990, pp. 1 s.

[112] Ad avviso di G. UBERTIS, *La prova penale*, cit., pp. 88 s. all'interno dei sistemi che rifuggono dalle prove legali può essere tracciata un'ulteriore linea di demarcazione. Da una parte vi sarebbero i sistemi basati sulla giuria, la quale emette un verdetto di carattere immotivato e facilmente influenzabile da tensioni emotive; dall'altra parte vi sarebbero i sistemi processuali che prevedono un convincimento razionale del giudice. Il nostro sistema apparterrebbe a quest'ultima categoria. Nello stesso senso, G. DE LUCA, *Profilo storico del libero convincimento del giudice*, in Aa. Vv., *Il principio del libero convincimento del giudice nel nuovo processo penale*, in *Quad. C.S.M.*, 1992, p. 38 ha definito il sistema emerso dal codice del 1988 come ispirato al libero convincimento motivato.

prova ammessa ed acquisita, per poi verificare se questa abbia raggiunto il livello di prova che la legge richiede.

Come anticipato, la questione fondamentale da affrontare ha ad oggetto quelli che sono i limiti alla libera valutazione della prova. Sul punto, la dottrina ha provveduto a chiarire il perimetro entro il quale può esplicarsi l'attività del giudice. Infatti, il legislatore, al fine di ricercare un giusto equilibro tra legalità e libertà nella valutazione delle prove, ha intesto garantire solo per quest'ultima fase una piena ed effettiva autonomia[113]. Viceversa, le altre tappe del procedimento probatorio sono precisamente scandite dalla legge, in applicazione del principio di legalità[114]. La conferma di un tale assunto è data dal fatto che possono formare oggetto di valutazione da parte del giudice solo ed esclusivamente le prove che sono state legittimamente ammesse e acquisite[115]. Infatti le prove assunte in violazione della legge sono dichiarate dallo stesso legislatore, all'art. 191 c.p.p., inutilizzabili.

Non solo: sempre al fine di garantire la corretta esplicazione del potere di apprezzamento delle prove, il codice di rito traccia una stretta linea di collegamento tra libero convincimento del giudice e obbligo di motivazione[116]. Questa tratto emerge a più livelli. Ad un più immediato esame, esso affiora dalla lettura combinata dell'art. 192 c.p.p. con le altre norme che si occupano della motivazione dei provvedimenti. Emblematico in tal senso è l'art. 546, co. 1°, lett. *e*) c.p.p., il quale impone al giudice di esplicitare i motivi di fatto e di diritto su cui si basa la sentenza, comprendendo in tale attività anche l'analisi delle prove a sostegno della

[113] F. IACOVIELLO, *La motivazione della sentenza penale e il suo controllo in cassazione*, Giuffrè, Milano, 1997, pp. 69 s. precisa come la libertà di decidere da parte del giudice sia, in ogni caso, una libertà secondo le regole che devono essere stabilite dalla legge circa il metodo da utilizzare in tale momento del procedimento probatorio.

[114] Cfr. M. NOBILI, *Art. 192*, in *Commento*, cit., pp. 415 s.

[115] La giurisprudenza, viceversa, sembra far riferimento ad un preteso principio di libertà della prova per cui sarebbero valutabili dal giudice tutti gli elementi probatori raccolti, v. *supra* nt. 71.

[116] Cfr. la *Rel. prog. prel. c.p.p.*, cit., p. 61 «decisamente nuovo è, però, il raccordo tra convincimento del giudice e obbligo di motivare: su un piano generale, esso mira a segnalare, anche a livello legislativo, come la libertà di apprezzamento della prova trovi un limite in princìpi razionali che devono trovar risalto nella motivazione».

decisione e di quelle contrarie. Dalla lettura della disposizione emerge uno schema di motivazione della sentenza ispirato senza dubbio al metodo dialettico[117]. Infatti nella sentenza il giudice è chiamato a fornire una duplice giustificazione. Da un lato, elencare quelle che sono le prove a favore della decisione presa; dall'altro lato, spiegare le cause per cui le prove contrarie alla decisione non possano condurre ad una diversa ricostruzione del fatto[118]. La ragione di un tale onere così particolare, va ricercata nella necessità di garantire che l'autorità giurisdizionale valuti tutte le prove che sono state ammesse. Così facendo, il legislatore ha inteso minimizzare la possibilità che il giudice potesse decidere in maniera completamente irrazionale, affidandosi esclusivamente al proprio intuito. Sul punto, sembra utile richiamare un'espressione usata da una dottrina tanto risalente quanto illustre, la quale affermava che «il giudice non ha vero arbitrio neppure dove si accetta l'intima convinzione; perché deve sempre convincersi secondo il processo e secondo ragione[119]». In questa breve citazione risulta compendiata la base su cui poggia l'attività di valutazione della prova: le risultanze probatorie emerse nel corso dell'istruzione dibattimentale e il pensiero razionale del giudice che, proprio perché basato sulla ragione, può, poi, essere espresso all'interno della motivazione del provvedimento.

Il secondo e più approfondito riguarda il collegamento sussistente tra alcuni degli elementi cardini del sistema processuale: il libero convincimento del giudice, l'obbligo di motivazione e il sistema delle impugnazioni. Infatti, come appena esplicitato, il convincimento

[117] A parere di G. UBERTIS, *La prova penale*, cit., p. 90, l'art. 546, co. 1° lett. *e*) c.p.p. «impone al giudice di seguire il metodo, tipico dell'epistemologia contemporanea, di coniugare il momento della conferma dell'ipotesi ricostruttiva accolta con quello della falsificazione delle ipotesi alternative respinte».

[118] Cfr. le precisazioni di R. APRATI, *Le prove contraddittorie:* id est *il diritto al contraddittorio sul medesimo tema probatorio*, in *Dir. pen. proc.*, 2006, p. 637, la quale sottolinea il rapporto sussistente tra contraddittorio e motivazione dialettica della sentenza.

[119] Cfr. F. CARRARA, *Programma del corso di diritto criminale. Parte generale*, Giusti, Lucca, 6° ed., 1886, § 886.

del giudice deve fondarsi su basi razionali: egli non decide mai sulla base del proprio intuito personale, ma deve essere in grado di fornire una spiegazione razionale della decisione presa. Questa evidentemente non può essere solo presente all'interno della mente dell'organo giudicante, ma deve essere esplicitata in una motivazione. Tuttavia, se, come chiarito dalla dottrina, quest'ultima serve a controllare la decisione, allora anche la motivazione deve essere verificabile. Lo strumento con cui si opera tale controllo è quello delle impugnazioni del provvedimento, ossia della possibilità che un altro giudice ripercorra l'*iter* motivazionale seguito dal primo al fine di vagliarne la correttezza. Questo dato si pone come elemento di chiusura del sistema che va ad evitare motivazioni apparenti, che sono superficialmente fondate su dati di carattere emozionale[120].

Sempre nell'ottica di guidare il convincimento del giudice, l'art. 192, co. 1° c.p.p. impone allo stesso di dar «conto nella motivazione dei risultati acquisiti e dei criteri adottati[121]». Con il primo termine il legislatore vuol fare riferimento all'esito dell'operazione probatoria compiuta. Pertanto, l'autorità giurisdizionale è chiamata a dar conto della coincidenza tra il fatto così come viene enunciato all'interno dell'atto di imputazione e la ricostruzione dello stesso per come emerge dalle prove che sono state ammesse e acquisite[122]. L'obiettivo perseguito dal legislatore è stato duplice. In primo luogo, saldare la decisione del giudice agli elementi probatori che sono stati introdotti dalle parti nel processo; in secondo luogo, garantire che il provvedimento non sia frutto della scienza privata del giudice[123].

[120] V. F. IACOVIELLO, *op. cit.*, pp. 67 s.

[121] M. NOBILI, *Art. 192*, cit., p. 416 lamenta l'esclusione nel testo finale dell'art. 192 c.p.p. del richiamo all'obiettività e alla prudenza nella valutazione della prova.

[122] Cfr. G. UBERTIS, *La prova penale*, cit., p. 28; E. FASSONE, *Dalla "certezza" all'"ipotesi preferibile": un metodo per la valutazione*, in *Riv. it. dir. proc. pen.*, 1995, p. 1111.

[123] In tal senso, v. G. DE LUCA, *Il sistema*, cit., p. 1259. In tema di scienza privata del giudice, la dottrina sottolinea come da questa nozione vada separata quella di fatti notori. Questi sono da intendere come tutti quei fatti che sono ritenuti dalle parti e dal giudice come fondati pur in difetto di prove a loro sostegno. Sul punto, v. G. UBERTIS,

Con il richiamo ai criteri adottati si pone, invece, l'accento sulle inferenze usate dal giudice per raggiungere un certo risultato probatorio. Come precisato dalla dottrina, le inferenze del giudice sono raggruppabili in tre categorie: quelle della logica, quelle della scienza e quelle della comune esperienza[124]. Queste ultime vanno a delimitare l'àmbito delle c.d. massime d'esperienza, ossia di quegli enunciati di carattere generale che collegano due classi di fatti sulla base del canone dell'*id quod plerumque accidit*[125]. Sul punto, il codice manifesta un atteggiamento di relativa prudenza. Infatti, da un lato, viene riconosciuto a questa fonte di conoscenza del giudice pieno valore. Ciò sulla considerazione per cui l'esclusione netta delle massime d'esperienza dagli strumenti conoscitivi del giudice impedirebbe allo stesso di giungere ad una decisione di carattere razionale[126]. Tuttavia, dall'altro lato, rendendosi conto delle insidie connesse ad un uso eccessivamente disinvolto delle massime d'esperienza, si richiede che quest'ultima sia esplicitata all'interno della motivazione della sentenza. Tale obbligo risulta funzionale al controllo circa la validità della regola d'esperienza utilizzata dal giudice. Infatti, come è stato sottolineato dalla dottrina, la possibilità di fondare un valido giudizio su di una massima d'esperienza dipende dal grado di concludenza della stessa. La funzione di questa limitazione è da ricercare nell'attenzione posta dal legislatore nell'evitare che «il libero convincimento divent[i] un grimaldello in mano al giudice *soi-pensant* onnisciente[127]».

La prova, cit., p. 36, il quale sottolinea come i fatti notori, pur non dovendo essere oggetto di prova, devono comunque essere resi noti alle parti al fine di garantire il contraddittorio tra le stesse.

[124] La suddivisione è proposta da P. FERRUA, *Il giudizio penale: fatto e valore giuridico*, in P. Ferrua – F.M. Griffantini – G. Illuminati – R. Orlandi, *La prova nel dibattimento penale*, Giappichelli, Torino, 4° ed., 2010, p. 354.

[125] Sul ruolo delle massime d'esperienza nelle valutazioni giudiziali, nella vigenza del codice del 1930, v. M. NOBILI, *Nuove polemiche sulle cosiddette «massime d'esperienza»*, in *Riv. it. dir. proc. pen.*, 1969, pp. 123 ss.

[126] In questi termini, G. UBERTIS, *La prova penale*, cit., p. 30.

[127] Così, F. CORDERO, *op. cit.*, p. 602

Nella cornice qui sommariamente delineata in relazione alla valutazione della prova, particolare attenzione deve essere posta, al fine del discorso che si sta conducendo, all'utilizzo da parte del giudice di prove scientifiche come fonte del proprio libero convincimento. Infatti, come sottolineato dalla dottrina, due sono le principali insidie che possono emergere. Da un lato, l'autorità giurisdizionale potrebbe essere tentata di sostituirsi agli esperti, diventando una sorta di «apprendista stregone[128]»; dall'altro lato, potrebbe, invece, affidarsi totalmente al perito, non effettuando alcun giudizio critico sulle conclusioni dello stesso[129].

Il principale antidoto contro tali pericoli è riconosciuto nell'inserimento della prova scientifica «nell'ordinaria epistemologia giudiziaria[130]». Il senso principale da attribuire ad una tale espressione è dato dalla necessità di valorizzare al meglio il contraddittorio, inteso nella duplice accezione di contraddittorio per la prova e sulla prova. Con la prima espressione si fa riferimento ad una partecipazione attiva al procedimento di formazione della prova, che avviene davanti al giudice del dibattimento a seguito dello scontro tra i due antagonisti del processo. Con la seconda, viceversa, si richiama l'idea per cui alle parti sia consentito di presentare all'organo giudicante le proprie argomentazioni e di essere ascoltati dallo stesso. Se il primo è il canone sancito dall'art. 111, co. 4°, il secondo è fissato dall'art. 111, co. 2° Cost.[131].

Guardando, in particolare, alla prova scientifica, quanto espresso in tema di contraddittorio può essere letto in un duplice senso. In primo luogo, dovrebbe essere valorizzato il

[128] Cfr., M. TARUFFO, *La prova dei fatti giuridici. Nozioni generali*, in *Trattato di diritto civile e commerciale*, già diretto da A. Cicu – F. Messineo, continuato da L. Mengoni, Giuffrè, Milano, 1992, vol. III, t. 2, sez. 1, pp. 309.

[129] In tal senso, v. C. CONTI, *La prova scientifica*, in *La prova penale*, a cura di P. Ferrua – E. Marzaduri – G. Spangher, Giappichelli, Torino, 2013, p. 107.

[130] Ancora, C. CONTI, *La prova scientifica*, cit., p. 107.

[131] In tema v., fra i tanti contributi, M. CHIAVARIO, *Giusto processo II) processo penale*, in *Enc. giur. Treccani*, Roma, 2001, p. 6.

contraddittorio tra i consulenti tecnici di parte[132]; in secondo luogo, l'esame del perito dovrebbe essere condotto con l'obiettivo di far emergere le specifiche competenze dell'esperto e la sua, eventuale, esperienza sul campo. In questo senso, appare criticabile la scelta di taluni giudici di nominare il perito scegliendolo dall'albo, senza un previo accertamento delle sue capacità e conoscenze particolari[133]. In terzo luogo, l'esame dovrebbe essere svolto sull'idoneità della tecnica scientifica scelta a fornire una ricostruzione del fatto che si intende provare. Infatti, davanti ad un perito particolarmente autorevole, il giudice potrebbe essere indotto ad affidarsi acriticamente alle sue conclusioni[134]. Il rispetto di queste brevi indicazioni dovrebbe fornire al giudice una valida piattaforma su cui esercitare in maniera razionale il proprio libero convincimento.

L'analisi, tuttavia, non può fermarsi all'individuazione di un'apprezzabile base valutativa per l'organo giurisdizionale. Infatti la dottrina – seguita dalla giurisprudenza – non ha mancato di delineare più precisamente gli indici e i criteri che dovrebbero essere seguiti in questo particolare segmento del procedimento probatorio dal giudice.

Alla base del discorso vi sarebbe un apparente paradosso[135]: il giudice richiede una perizia proprio perché riconosce la propria incapacità di governare la prova scientifica. Tuttavia, essendo egli *peritus peritorum* è chiamato a valutare l'operato dell'esperto. Sembrerebbe, quindi, che la prova scientifica sia destinata ad introdurre nel processo del materiale difficilmente valutabile. Infatti l'autorità giurisdizionale si troverebbe nella difficile posizione di dover analizzare criticamente il compimento di una serie di operazioni effettuate

[132] Cfr., C. CONTI, Iudex peritus, cit., p. 33, la quale, inoltre, auspica, *de iure condendo*, l'introduzione dell'obbligo di verità per i consulenti tecnici e la possibilità che questi partecipino attivamente all'esame degli altri consulenti o del perito. In senso adesivo, v. S. LORUSSO, *op. cit.*, p. 335.

[133] Così. C. CONTI, Iudex peritus, cit., p. 34

[134] Cfr. C. CONTI, Iudex peritus, cit., p. 34

[135] Il riferimento è al paradosso individuato da M. TARUFFO, *La prova scientifica*, cit., pp. 1109 s.

proprio sul presupposto della sua ignoranza della materia. L'impossibilità di poter pienamente sottoporre a critica le operazioni compiute da un perito, ha portato alcuni Autori a sottolineare il pericolo che la perizia si trasformi in una sorta di prova legale[136]. Infatti il giudice, non essendo in grado di porre fondatamente in dubbio quanto affermato dall'esperto, finirebbe per seguire ciecamente il suo parere.

In realtà, la dottrina più attenta non ha mancato di precisare come l'opera di valutazione della prova scientifica non sia sottratta al libero convincimento del giudice. Quest'ultimo, infatti, non è chiamato a ripercorrere passo dopo passo le operazioni del perito alla ricerca di errori sperimentali[137]. Più correttamente, si richiede all'organo giurisdizionale una valutazione di carattere metodologico, finalizzata all'analisi dell'attendibilità del parere dell'esperto. In soccorso del giudice giungerebbe quella che è stata definita dalla dottrina «cultura di criteri[138]». Alla base di una tale ricostruzione vi sarebbe il rilievo per cui differente sarebbe la cultura da impiegare nella ricostruzione del fatto e in quella della valutazione della prova scientifica. Per il primo, dovrebbe essere impiegata quella che viene definita la cultura di merito. Questa consiste in nozioni generali, regole d'esperienza e leggi scientifiche che fanno ormai parte del sapere comune. Per la seconda, invece, si dovrebbe utilizzare la cultura di criteri. Questa contiene schemi concettuali di valutazione della validità del metodo scientifico che possano permettere di controllare l'affidabilità delle conclusioni dell'esperto[139]. L'individuazione di tali criteri è lasciata al giudice, il quale in quest'opera di

[136] In tal senso si è espresso, G. F. RICCI, *Nuovi rilievi sul problema della «specificità» della prova giuridica*, in *Riv. trim. dir. proc. civ.*, 2000, p. 1154.

[137] V., C. BRUSCO, *La valutazione della prova scientifica*, in *La prova scientifica*, cit., p. 28.

[138] L'espressione è di O. DOMINIONI, *La prova penale*, cit., pp. 69 ss.

[139] Cfr. O. DOMINIONI, *La prova penale*, cit., p. 69.

definizione dei parametri più opportuni per valutare la prova scientifica può fare riferimento alla stessa giurisprudenza, all'elaborazione dottrinale su certi strumenti probatori, ai contributi della scienza[140]. Ovviamente, questo lavoro di ricerca dovrebbe essere esplicitato dal giudice nella motivazione della sentenza, all'interno della quale devono essere indicati tutti i parametri utilizzati. La funzione di una tale attività è da ricercare nella logica del controllo e della formazione di un'ampia cultura di criteri. Infatti attraverso il sistema delle impugnazioni è possibile controllare la validità delle scelte operate dal giudice e, espandendo l'orizzonte oltre il singolo caso, sviluppare una più ampia cultura di criteri.

In questa opera di selezione delle regole da seguire nella valutazione della prova scientifica, possono essere ulteriormente richiamati i contributi forniti sul tema dalla giurisprudenza nordamericana[141].

Volendo essere più analitici sul punto, merita di essere segnalata l'opinione di chi ritiene che la valutazione della prova scientifica debba articolarsi in due tempi[142]. Il primo momento avrebbe ad oggetto l'analisi del risultato di prova raggiunto attraverso l'opera dell'esperto; il secondo comporterebbe, invece, una valutazione generale di tutte gli elementi probatori utilizzabili dal giudice.

In altri termini, nel primo livello della valutazione della prova scientifica, il giudice sarebbe chiamato a svolgere la funzione di «*gatekeeper*» della stessa nel processo penale[143]. Nella funzione di guardiano, il giudice è chiamato a controllare l'idoneità probatoria del mezzo impiegato. Questa verifica impone, di conseguenza, quella sulla validità teorica della

[140] V. O. DOMINIONI, *La prova penale*, cit., p. 71.

[141] Si rimanda, sul punto, alle considerazioni effettuate *supra* al § 1.

[142] O. DOMINIONI, *La prova penale*, cit., pp. 297 s.

[143] Cfr. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, cit., 597, la quale, tuttavia, impone che tale funzione sia svolta nel momento ammissivo della prova e non in quello valutativo.

tecnica scientifica utilizzata. In questa fase, il giudizio effettuato dall'organo giurisdizionale avrebbe un valore diverso rispetto a quello compiuto in fase di ammissione della prova. Questo, infatti, sarebbe da intendersi come conclusivo in punto di correttezza scientifica del metodo[144]. L'obiettivo da raggiungere sarebbe quello di evitare che il giudice si appiattisca sulle opinioni degli studiosi, accettando acriticamente le stesse[145]. Per raggiungere un tale traguardo, secondo alcuni il giudice potrebbe anche disporre un'ulteriore perizia con un duplice scopo. Da un lato, avere un'ampia visione del panorama scientifico sul tema e, dall'altro, sottoporre a critica l'operato di un altro esperto[146].

Appurata la validità teorica della metodologia impiegata durante il processo, si dovrebbe passare, prosegue questa dottrina, al controllo circa l'adeguatezza dello strumento utilizzato alla ricostruzione del fatto oggetto di prova. Si tratta, in sostanza, di calare nella concreta realtà processuale la tecnica impiegata andando a verificare che questa sia, usando un termine della giurisprudenza nordamericana prima citata, «*fit*» rispetto ai fatti da accertare[147].

La soluzione positiva di tale incombente porta al successivo *step* della valutazione della prova scientifica, il quale è rappresentato dall'esame circa la corretta applicazione del metodo da parte dell'esperto. In altri termini, dopo aver accertato che la prova acquisita si basi su metodi astrattamente corretti e che questa possa fornire elementi utili per la decisione, l'organo giurisdizionale è chiamato a saggiare il comportamento tenuto dall'esperto.

[144] Cfr. O. DOMINIONI, *La prova penale*, cit., pp. 298 ss.

[145] Così, O. DOMINIONI, *La prova penale*, cit., pp. 297 s.

[146] In tal senso, C. CONTI, Iudex peritus, cit., p. 34; L. LOMBARDO, *La scienza e il giudice nella ricostruzione del fatto*, in *Riv. dir. proc.*, 2007, p. 51.

[147] V. *supra* § 1.

Questo risulta essere uno dei momenti centrali della valutazione della prova scientifica; infatti, molto spesso i maggiori errori si verificano proprio a causa di un errato uso della metodologia scientifica prescelta dal perito o dal consulente tecnico. In questa sotto-fase, due sono i principali campi in cui si sviluppa l'opera di accertamento descritta[148]. In prima battuta, nella verifica circa la correttezza dei dati di cui si è avvalso lo specialista; in seconda battuta, nella giusta applicazione nel caso concreto di tutti i princìpi, i metodi e gli strumenti che vengono in gioco. Inoltre, andrebbero appurate tanto la «completezza[149]» quanto la «comprensione[150]» della prova scientifica. Se con la prima espressione si fa riferimento all'impiego da parte del perito o del consulente tecnico di tutti i dati a sua disposizione, in quanto, un uso parziale degli stessi potrebbe facilmente condurre a risultati errati. Con la seconda si allude all'idea per cui il giudice deve essere in grado di comprendere il grado di affidabilità e di validità della prova scientifica che egli è chiamato a valutare.

Il secondo stadio, viceversa, abbraccia una prospettiva nettamente diversa. Questo, infatti, va a cogliere il fenomeno della prova scientifica nuova in relazione a tutte le prove che sono state assunte durante l'istruzione dibattimentale. In tale fase, il giudice è chiamato, grazie all'utilizzo di criteri logici, esperienziali e tecnico-scientifici propri del sapere comune, a fornire una valutazione generale di tutto il materiale probatorio che ha a disposizione allo scopo di giungere ad una decisione finale circa la fondatezza o meno dell'imputazione.

Così ricostruito il quadro della dottrina, risulta utile uno sguardo alla giurisprudenza. In relazione al discorso che si sta conducendo circa la valutazione della prova scientifica nuova, deve essere sottolineato come un punto di svolta della materia sia rintracciabile in

[148] V., O. DOMINIONI, *La prova penale*, cit., pp. 301 s.

[149] Ancora, O. DOMINIONI, *La prova penale*, cit., pp. 303 s.

[150] Così, O. DOMINIONI, *La prova penale*, cit., pp. 304 s.

una sentenza relativamente recente[151]. La principale questione da risolvere nella sentenza in commento aveva ad oggetto la sussistenza o meno di un nesso causale tra l'esposizione di alcuni operai – alcuni dei quali poi deceduti – alle polveri d'amianto e l'insorgere della patologia denominata mesotelioma pleurico. Oltre che per l'aspetto relativo alla sussistenza del nesso causale, che esula dal tema del presente lavoro, la sentenza citata risulta estremamente interessante perché è la prima volta che in Italia vengono espressamente richiamati i criteri della già citata sentenza *Daubert*[152]. La questione che il giudice si trovava a risolvere era controversa. Infatti all'interno della comunità scientifica vi è un dibattito circa i rapporti tra esposizione all'amianto ed insorgenza del mesotelioma pleurico[153]. Il giudice si trovava, quindi, ad inserirsi in un dibattito scientifico controverso e a dover scegliere una delle tue tesi. Al riguardo, va ricordato come, secondo l'orientamento prevalentemente accettato dalla giurisprudenza di legittimità, il giudice sia libero di scegliere la teoria che più lo convinca, purché nella motivazione della sentenza dia conto in maniera chiara e approfondita della sua scelta[154]. Questa prospettiva è stata criticata da molti in dottrina, rilevando come, nella maggior parte dei casi, il principio del libero convincimento del giudice sia usato come un paravento per giustificare decisioni basate solo sulle risultanze della perizia[155].

Nel caso di specie la Corte accoglie una prospettiva nettamente differente. Nella sentenza, infatti, si legge che per valutare l'attendibilità di una teoria sia necessario esaminare gli studi che la sorreggono; le basi fattuali sui quali questi sono condotti. Non solo, l'ampiezza,

[151] Cfr. Cass. sez. IV, 17 settembre 2010, Cozzini, cit., pp. 1341 ss. Nello stesso senso, v. Cass. sez. IV, 29 gennaio 2013, Cantore, cit.

[152] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, cit.,

[153] Per una breve panoramica delle tesi scientifiche riguardanti il nesso causale tra esposizione all'amianto ed insorgenza del mesotelioma pleurico, v. S. ZIRULIA, *Amianto e responsabilità penale: causalità ed evitabilità dell'evento in relazione alle morti derivate da mesotelioma pleurico*, in *www.penalecontemporaneo.it*

[154] Cfr., tra le ultime pronunce di tale orientamento, Cass. sez. IV, 13 febbraio 2015, Sartori, in *C.e.d. cass.* n. 263435.

[155] In tal senso, v. G. GENNARI, *Scienziati e giudici: l'incontro (im)possibile*, in *Medicina e diritto*, 2010, f. 3, p. 7.

la rigorosità e l'oggettività della ricerca; il grado di sostegno che i fatti accordano alla tesi. Inoltre, deve anche essere tenuta in conto la discussione che ha accompagnato l'elaborazione dello studio, focalizzando l'attenzione sia sui i fatti che mettono in discussione l'ipotesi sia sulle diverse opinioni che si sono formate nel corso della discussione. Da ultimo, merita attenzione l'attitudine esplicativa dell'elaborazione teorica, il grado di consenso che la tesi raccoglie nella comunità scientifica di riferimento e l'autorevolezza, l'indipendenza di chi svolge la ricerca e le sue finalità. Passando da una valutazione in astratto ad una in concreto, la sentenza prosegue affermando come, valutata l'affidabilità metodologica di una certa teoria, diventa poi necessario controllare che essa sia in grado di fornire concrete e significative informazioni idonee a sorreggere l'argomentazione probatoria del caso specifico. Quando si registra un contrasto scientifico, il compito dell'esperto non è quello di fornire la soluzione del contrasto al giudice. Ma, piuttosto, di dare a quest'ultimo contezza del dibattito in corso e di fornirgli le nozioni minime per permettere al giudice una scelta circa la teoria che possa meglio spiegare il caso concreto[156].

Emergono, già ad una prima lettura, forti e chiari riferimenti alla giurisprudenza nordamericana in tema di prova scientifica[157]. Rispetto a questi, si registra, però, nella decisione in commento un'importante aggiunta: la valutazione circa l'indipendenza tanto dello studioso quanto dello studio che si intende utilizzare come mezzo di prova.

Questo passaggio argomentativo della sentenza è stato sottoposto a critica. Infatti la valorizzazione della libertà di pensiero e degli scopi che portano l'esperto ad intervenire nel processo potrebbe condurre ad una sopravvalutazione dell'opera del perito rispetto a quella

[156] Cfr. Cass. sez. IV, 17 settembre 2010, Cozzini, cit., pp. 44 ss.

[157] Precedentemente, un accenno alle già citate sentenze della Corte suprema degli Stati Uniti d'America viene fatto, seppur brevemente, in Cass. sez. I, 21 maggio 2008, Franzoni, cit. In questa pronuncia i giudici affermano come i criteri elaborati dalla Corte suprema possano avere solo un valore orientativo per il giudice italiano.

del consulente tecnico[158]. Soltanto il primo, infatti, non avendo un interesse diretto riguardo ai fatti da accertare sembrerebbe essere effettivamente libero da ogni pregiudizio. Invero, una tale impostazione pare da respingere alla luce proprio del discorso che è stato condotto in queste pagine. Infatti nel momento in cui si accerta il disincanto della scienza moderna e si ammette un contraddittorio sulla e per la prova scientifica, allora tutti i contributi degli esperti devono essere posti sullo stesso piano[159]. Non solo, come fatto notare da un'attenta dottrina, la prova apparentemente neutra risulta, in effetti, la più insidiosa da valutare. Solo conoscendo l'interesse di cui la parte si fa portatrice, il giudice può valutare serenamente il contributo fornito. La perizia, soprattutto quando le parti non nominano loro consulenti tecnici, rischia di rivelarsi un mezzo di prova estremamente più scivoloso di quanto non possa sembrare. Ciò perché il canone di neutralità che accompagnerebbe l'escussione del perito potrebbe indurre il giudice ad abbassare la guardia e a non valutare correttamente il risultato della sua attività[160].

[158] V. quanto precisato da D. VICOLI, *Riflessioni sulla prova scientifica: regole inferenziali, rapporti con il sapere comune, criteri di affidabilità*, in *Riv. it. med. leg.*, 2013, pp. 1251 s.

[159] In tal senso, v. D. VICOLI, *op. cit.*, pp. 1152 ss.

[160] Cfr. C. CONTI, iudex peritus, cit., p. 35.

Capitolo II

La definizione di prova di carattere informatico

Sommario: 1. Caratteri generali della digital evidence *– 2. La definizione di fonte di prova informatica – 3. La* digital evidence *come documento informatico – 4. La* digital evidence *come flusso di dati*

1. Caratteri generali della *digital evidence*

Prendendo le mosse da un'ovvia considerazione, si può affermare come la nostra esistenza si sia sempre più digitalizzata: uno sguardo all'indietro, nel recentissimo passato, può essere utile per rilevare l'espansione dell'informatica nella nostra vita quotidiana. Il *computer*, nato come strumento pensato per effettuare calcoli matematici, è diventato, successivamente, un oggetto di comune utilizzo in àmbito lavorativo. Non solo: l'informatica e le nuove tecnologie sono uscite dagli uffici per trasformarsi in un elemento costante della nostra realtà. Infatti, soprattutto negli ultimi dieci anni, i dispositivi elettronici nelle loro varie declinazioni sono diventati normali strumenti di interazione nella vita sociale. Dall'utilizzo del *computer* in ambiente lavorativo, si è giunti all'impiego dei *personal computer*, dei *tablet*, degli *smartphone* in àmbito domestico. A rendere più capillare l'uso dei dispositivi elettronici ha contribuito un altro fattore legato all'evoluzione tecnologica: la diffusione di *Internet* e del *World Wide Web*. Infatti la creazione di una rete tra *computer* che consentisse il rapido scambio di informazioni tra utenti è passata, in un periodo relativamente breve, da essere uno

strumento pensato per lo scambio di dati tra ricercatori ad essere uno mezzo di comunicazione di massa. Questo ha permesso, tra le altre cose, la nascita del c.d. *social web*, ossia di quell'insieme di piattaforme che permettono agli utenti di interagire tra di loro.

Il risultato raggiunto dal combinato dei due fattori appena descritti non è, ovviamente, indifferente per il mondo giuridico e, soprattutto, per quello del processo penale. Infatti gli strumenti digitali sono in grado di trattenere un gran numero di dati sull'utente che li utilizza; informazioni che possono rivelarsi estremamente importanti in un'indagine penale[1]. La grande rilevanza di questi elementi per l'accertamento di un reato ha portato alcuni a ritenere che l'ingresso dell'informatica nei procedimenti penali rappresenti un momento di profondo cambiamento del processo, pari all'introduzione dell'istruttoria medievale[2].

Nel contesto brevemente tratteggiato si inserisce l'oggetto del presente lavoro: la *digital evidence*. Tuttavia, prima di proseguire nella trattazione, è opportuna una prima puntualizzazione. Tradizionalmente il tema delle prove di carattere digitale è stato trattato in relazione ai *computer crimes*, ossia a quei delitti che vengono commessi attraverso l'utilizzo di un calcolatore[3]. In realtà, proprio lo sviluppo delle nuove tecnologie ha ampliato la portata del tema rendendolo, di fatto, trasversale ad ogni procedimento penale, nel quale le parti

[1] È, comunque, necessario precisare, come fanno molti Autori, che le indagini informatiche da sole difficilmente possono portare a risultati utili per l'accertamento di un illecito. Infatti, una volta tracciato un collegamento tra un reato e un dispositivo elettronico si pone la questione circa l'identità del soggetto che lo ha effettivamente utilizzato. Sul punto, tra i tanti si rimanda a L. LUPÁRIA, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, in L. Lupária – G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007, p. 144.

[2] L'affermazione, espressa originariamente da G. ALESSI, *Il processo penale. Profilo storico*, Laterza, Bari, 2001, p. 180, è ripresa da L. LUPÁRIA, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in L. Lupária – G. Ziccardi, *op. cit.*, p. 134.

[3] La l. 23 dicembre 1993, n. 547 è stata la prima a regolare il fenomeno dei reati informatici. Con tale locuzione la dottrina penalistica fa riferimento a quella serie di fattispecie penali caratterizzate da una triplice connessione con l'informatica. In primo luogo, il collegamento può manifestarsi in relazione alla condotta dell'agente, il quale utilizza il *computer* come strumento con il quale si commette un crimine. Inoltre, il sistema informatico può costituire l'oggetto materiale del reato. Infine, il legame tra diritto penale e informatica si manifesta in relazione all'esigenza di tutelare nuovi beni giuridici come quello della sicurezza informatica. V., più diffusamente, L. PICOTTI, *Reati informatici*, in *Enc. giur. Treccani*, Roma, 1999, p. 2.

possono avere la necessità di estrarre dati da un *device* elettronico. Questi possono essere utilizzati, ad esempio, dalla difesa per provare un alibi. Uno dei casi in questo senso più noti è sicuramente quello realizzatosi nell'àmbito del procedimento avviato per l'omicidio di Chiara Poggi. L'imputato, Alberto Stasi, basava, infatti, parte della propria strategia difensiva su di un alibi informatico[4]. Egli affermava di non poter essere l'autore del reato, in quanto all'ora in cui si sarebbe verificata l'aggressione stava lavorando alla propria tesi sul proprio *personal computer*.

Da un'altra ed opposta visuale, può essere l'accusa ad aver interesse a recuperare importanti documenti, tali da corroborare l'ipotesi accusatoria. Al riguardo, può citarsi, emblematicamente la vicenda dei documenti trovati nei palmari degli appartenenti al gruppo terroristico delle nuove Brigate rosse[5].

Questa prospettiva, che è stata brevemente delineata, è quella prescelta per il presente lavoro: alla luce della pervasività dell'informatica nella vita di tutti i giorni, il tema delle prove di carattere informatico sarà analizzato partendo dall'idea per cui questo tipo di materiale probatorio sia una fondamentale risorsa per le parti in tutte le indagini di carattere penale.

Per muoversi all'interno del vasto universo della "prova informatica" è necessario compiere alcune precisazioni. La prima, di carattere tecnico, ha ad oggetto il nome stesso da attribuire alla materia da trattare. Come chiarito da alcuni, appare ormai più corretto fare riferimento al termine *digital forensics* rispetto che a quello di *computer forensics*[6]. Questo

[4] Cfr., tra le tante, la ricostruzione offerta da E. COLOMBO, *La sentenza del caso di Garlasco e la* computer forensics*: analisi di un complesso rapporto tra diritto ed informatica*, in *Cyberspazio e diritto*, 2010, pp. 447 ss.

[5] V. le motivazioni di Cass. sez. I, 27 giugno 2007, Lioce ed altri, in *C.e.d. cass.* n. 237768.

[6] Così, A. GHIRARDINI – G. FAGGIOLI, Digital forensics, Apogeo, Milano, 3° ed., 2013, p. 2.

perché l'innovazione tecnologica ha fuso due delle principali branche dell'informatica forense: la *computer forensics* e la *network forensics*. Fino a pochi anni fa, con la prima si intendevano quelle tecniche di analisi di dati immagazzinati su di un determinato sistema, come poteva essere il *computer* dell'indagato; con la seconda quelle metodologie finalizzate alla raccolta di dati transitanti all'interno di reti. Attualmente, lo sviluppo del c.d. *cloud computing* ha reso questa distinzione superata, in quanto i dati utili per un'indagine sono quelli che derivano dall'analisi combinata di ciò che si trova su di un elaboratore e di quelli transitati nella rete cui il *computer* è connesso[7].

Oggetto principale di studio della *digital forensics* è il dato informatico. Questo è costituito da una sequenza di 0 e 1, i quali costituiscono il c.d. linguaggio macchina, ossia la lingua effettivamente compresa dai microprocessori. L'informazione minima processabile da un elaboratore è definita *bit*, abbreviazione di *binary digit*. Il linguaggio macchina è stato codificato, assegnando ad una certa sequenza di 0 e 1 un determinato simbolo. Allo stato, la codifica che funge da standard è quella denominata ASCII[8]. Altra caratteristica fondamentale del dato informatico è la sua immaterialità: qualsiasi strumento elettronico è composto da una parte fisica, l'*hardware* e da una parte logica, il *software*. Questa seconda è sostanzialmente priva di corporeità, comportando, come ulteriore conseguenza, la sua autonomia rispetto al supporto dove essa è contenuta[9].

[7] Si pensi al caso in cui l'utente utilizzi un servizio di *cloud* pubblico come *Dropbox*: i dati effettivamente contenuti sul dispositivo possono essere irrilevanti o di scarso valore per un'indagine. Tuttavia, estendendo il campo dell'analisi anche a quanto il soggetto detiene sul proprio spazio di archiviazione *on-line*, risulterà possibile accedere a elementi particolarmente significativi che l'utente ha deciso di cancellare dal *device* e di mantenere solo sulla "nuovola".

[8] Acronimo di *American Standard Code for Information Interchange*, pubblicato nel 1968 dall'*American National Standards Institute*, un'associazione che si occupa di definire gli *standard* industriali per gli Stati Uniti d'America.

[9] Sicuramente il dato informatico non può esistere senza un supporto idoneo ad immagazzinarlo, tuttavia, questo può essere, appunto, facilmente duplicato e spostato su di un altro supporto equivalente. Inoltre, va precisato come sia il *software* sia le informazioni da esso elaborati costituiscono dati informatici.

Il dato informatico è un'entità alquanto particolare, dotata di caratteristiche sue peculiari. In particolare, esso appare, ad un tempo estremamente fragile e facilmente duplicabile. Infatti l'informazione immagazzinata su di un supporto può essere facilmente modificata o danneggiata sia volontariamente sia involontariamente. Per questo motivo, è noto come gli esperti consiglino la massima prudenza nel maneggiare dati informatici: un'operazione audace potrebbe portare, infatti, a rovinare in maniera irreparabile il dato informatico[10]. Tuttavia, questa fragilità risulta essere in un certo senso controbilanciata dalla proprietà che più distingue il dato informatico da qualsiasi altro elemento: la sua riproducibilità. Infatti la sequenza di *bit* presente su di un supporto può essere facilmente duplicata, ottenendo due *files* assolutamente identici sotto ogni aspetto[11].

Non solo, un'altra qualità delle informazioni contenute in un sistema informatico che in qualche misure bilancia la loro fragilità è la pervasività della loro raccolta. Qualsiasi strumento informatico contiene un grandissimo numero di informazioni, molto spesso archiviate o conservate all'insaputa dell'utente che lo utilizza. Queste informazioni rivestono, ovviamente, una grande importanza per le indagini informatiche. Un esempio che può valere a chiarire questa affermazione è quello concernente il c.d. *file slack*. Quando viene cancellato un *file* da un qualsiasi *device* elettronico, questo non viene, di norma, immediatamente distrutto dal sistema. Infatti, a seguito del comando volto alla cancellazione del dato, il sistema non fa altro che segnare come libero lo spazio in cui è allocato il *file* che si vuole eliminare.

[10] Ad esempio, A. GHIRARDINI – G. FAGGIOLI, *op. cit.*, p. 89 rilevano come il collegamento di un qualsiasi *hard disk* esterno ad un *computer* che utilizza il sistema operativo *Windows* comporti un'automatica scrittura di alcuni dati sul supporto. Tale automatismo, pensato per facilitare l'utilizzazione dell'elaboratore da parte dell'utente medio, richia di rendere lo stesso irrimediabilmente inutilizzabile in sede processuale. Dal momento che, l'*hard disk* "corrotto" non costituirebbe più, infatti, una fedele copia di quello sequestrato, non potrebbero che derivare fondati dubbi sulla genuinità dei dati eventualmente estratti.

[11] Proprio questa caratteristica rende impossibile un furto, in senso classico, di un *file*. Cfr. A. GHIRARDINI – G. FAGGIOLI, *op.cit.*, p. 5. In giurisprudenza, Cass. sez. IV, 26 ottobre 2010, Petrosino, in *C.e.d. cass.* n. 249067 ha escluso la configurabilità del furto in caso di copiatura non autorizzata di un *file* da un supporto informatico altrui.

L'effettiva distruzione del *file* si ha soltanto quando il sistema riscrive quella porzione del supporto, sostituendo al vecchio *file* cancellato uno nuovo. Questa particolarità del funzionamento del sistema di archiviazione delle informazioni dei dispositivi elettronici può essere estremamente rilevante per un inquirente, il quale, attraverso l'utilizzazione degli opportuni *tool* informatici, dispone della possibilità di recuperare parzialmente o interamente un *file* che l'utente credeva, erroneamente, di aver cancellato.

Tuttavia, come già scritto, alle grandi moli di dati raccolti se ne collega la loro estrema fragilità. Proprio tale ultima caratteristica rende fondamentale l'utilizzo di opportune tecniche di raccolta delle informazioni da un elaboratore. Sul punto, vi è una tendenziale comunanza di opinioni circa l'utilizzo della c.d. *bitstream image*[12]. Con questa espressione si fa riferimento ad una tecnica di copiatura dei supporti informatici in grado di copiare tutti i *bit* di un determinato supporto su di un altro. Il risultato finale dell'operazione esperita è quello di avere due supporti informatici assolutamente identici da un punto di vista logico. L'importanza di una copiatura completa di tutto un *hard disk* può essere compresa alla luce dell'esempio fatto appena prima in tema di *file slack*. Infatti solo a seguito di una duplicazione completa è possibile analizzare anche le parti "vuote" del supporto informatico alla ricerca di fondamentali informazioni che magari l'utente voleva nascondere. Vista l'importanza di avere una copia assolutamente identica, fondamentale diventa parimenti la questione di come controllare l'identità tra due supporti. Anche su questo fronte, gli Autori concordano circa l'importanza dell'utilizzo di funzioni di *hash* al fine di validare il procedimento di copiatura. Queste funzioni operano come una *black box* nella quale, inserito un qualsiasi *input*,

[12] Tra gli altri, si esprimono a favore dell'utilizzo della *bitstream image* come metodo di copiatura dei supporti informatici S. ATERNO, Digital forensics *(investigazioni informatiche)*, in *Dig. pen.*, Utet, Torino, 2014, agg. VIII, p. 219; L. LUPÁRIA, *La ricerca*, cit., p. 152; L. MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4519; F. M. MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2010, p. 1266.

si otterrà un *output* standard chiamato *fingerprint*, impronta. Una minima modificazione dell'*input* condurrà ad un *output* completamente diverso[13]. Solo se le due impronte dei *files* corrispondono, allora si potrà essere certi della loro perfetta identità[14].

[13] Un'applicazione pratica di una delle funzioni di *hash* più usate, l'md5, varrà a chiarirne il funzionamento. Questa funzione, per qualsiasi *input*, consegna un *output* di 128 *bit*. Se si fornisce l'*input* «Cantami o diva l'ira funesta del pelide Achille», l'*output* sarà 567803d73b51108b34536dbdd0c75951. Cambiando una sola lettera e fornendo quindi l'*input* «Contami o diva l'ira funesta del pelide Achille», l'*output* sarà e4f58b225482bf42217eee1dd12a9254. Come si vede, il semplice cambiamento di una sola lettera ha generato una sequenza completamente diversa di caratteri.

[14] Allo stato, deve essere segnalato come non esista alcuna funzione di *hash* in grado di garantire che a due *input* diversi vi siano sempre due *output* diversi. Per questo motivo, in sede di raccolta di *digital evidence* si preferiscono utilizzare due funzioni di *hash*, in modo da ridurre al minimo eventuali errori.

2. La definizione di fonte di prova informatica

Delineati sommariamente i tratti qualificanti il dato informatico, occorre ora porre l'attenzione sulla definizione di *digital evidence*. Una prima enunciazione è quella fornita da uno dei più importanti studiosi del tema a livello internazionale, il quale definisce la *digital evidence* come «*any data stored or transmitted using a computer that support or refute a theory of how an offence occurred or that address critical elements of the offence such as intent or alibi*[15]». Sulla stessa linea si pone la *Guida alla prova digitale* realizzata all'interno di un progetto di cooperazione contro la criminalità informatica in àmbito europeo[16]. Questa, infatti, definisce le *digital evidence* come quelle «fonti di prova che sono utilizzate in un procedimento giudiziario e che derivano da dispositivi elettronici come i computer e le relative periferiche, le reti di computer, i telefoni cellulari, le fotocamere digitali o altri dispositivi mobili, i dispositivi di archiviazione dati, nonché da Internet[17]». Entrambi i testi concentrano la loro attenzione sul dato informatico in quanto tale, sottolineandone la sua connessione con l'accertamento di un illecito. In una prospettiva non dissimile si pongono alcuni studiosi italiani, i quali, dopo aver definito i crimini informatici come quegli illeciti commessi tramite un *computer*, diretti ad un *computer* oppure in cui un elaboratore rappresenta una fonte di

[15] E. CASEY, *Digital evidence and computer crime. Forensic science, computer and the internet*, Academic Press, Cambridge, Massahussets, 3° ed., 2011, p. 7.

[16] Più precisamente, la necessità della formazione di un testo europeo di riferimento per l'analisi delle fonti di prova digitali è emersa, per la prima volta, all'interno di un progetto di cooperazione tra Unione europea e Consiglio d'Europa finalizzato alla lotta al *cybercrime* in Paesi desiderosi di diventare membri dell'Unione europea. Per un approfondimento del progetto, si rimanda al sito *web* dello stesso: http://www.coe.int/en/web/cybercrime/cybercrime-ipa

[17] Cfr. *Guida alla prova digitale. Linee guida per la polizia giudiziaria e autorità giudiziaria*, versione 1.0, p. 12.

prova, proseguono intendendo la *computer forensics* come quell'insieme di attività finalizzate alla risoluzione dei casi connessi alla criminalità informatica[18]. Un'altra parte della dottrina, invece, pur focalizzando la propria attenzione sul dato informatico ne sottolinea un altro aspetto. Infatti la *computer forensics* sarebbe quella scienza che è in grado di studiare il valore che un certo dato informatico può avere in àmbito giuridico. In quest'ottica, il concetto di valore viene declinato in senso processuale, intendendolo come la capacità di resistenza di un dato informatico alle contestazioni delle altre parti processuali[19].

Le definizioni appena proposte, pur essendo valide dal punto di vista tecnico informatico, risultano essere eccessivamente generiche da quello giuridico, soprattutto se rapportate agli istituti propri del codice di procedura penale. Il rischio derivante dall'accettazione delle definizioni appena fornite sarebbe quello di vedere prove informatiche dovunque, di confondere, ad esempio, le fonti di prova digitali con i risultati delle intercettazioni "classiche"[20].

La necessità di effettuare un'opera di ridefinizione dei confini tra *digital evidence* e prove tradizionali nasce da almeno tre fattori. In un'ottica generale e di ampio respiro, risulta centrale la capillare informatizzazione della nostra società. Conseguenza di tale fenomeno è la digitalizzazione di gran parte del materiale probatorio. Infatti sembra possibile immaginare in un prossimo futuro un processo penale interamente digitalizzato nel quale tutti gli atti processuali siano documenti informatici[21]. Non solo, l'avanzare dell'informatica ha ripercussioni anche sugli istituti "classici" del codice di rito penale. Infatti la digitalizzazione dei

[18] Cfr. C. MAIOLI, *Dar voce alle prove: elementi di Informatica forense* consultabile all'indirizzo http://www.informaticaforense.it/diario/a-a-2010-2011.html

[19] V. G. ZICCARDI, *Scienze forensi e tecnologie informatiche*, in L. Lupària – G. Ziccardi, *op. cit.*, pp. 4 s.

[20] In tal senso, v. G. DI PAOLO, *Prova informatica (diritto processuale)*, in *Enc. dir.*, Giuffrè, Milano, 2013, ann. VI, p. 739.

[21] Cfr. G. ZICCARDI, *op. cit.*, p. 9. Si rimanda a G. DE RUGERIIS, *Effetti delle innovazioni tecnologiche sul processo penale*, in *Questioni di informatica forense*, a cura di C. Maioli, Aracne, Roma, 2015, pp. 89 ss. per una ricostruzione degli interventi finalizzati all'informatizzazione del processo penale.

servizi di telefonia va a porre in crisi la distinzione tra i mezzi di comunicazione tradizionali e quelli moderni. Ad oggi, qualsiasi telefonata è riconducibile ad un flusso di dati digitali. Alto è, quindi, il rischio di attrarre nell'orbita delle *digital evidence* tutta la materia delle intercettazioni[22]. Da ultimo, la diffusione dell'informatica di consumo nella nostra società ha comportato una rapida e piena propagazione di strumenti elettronici. Questi possono rivestire ruoli diversi rispetto ad un'indagine penale, potendo essere alternativamente il mezzo per compiere un delitto, il dispositivo usato a fini investigativi dagli inquirenti oppure il deposito di informazioni afferenti al suo utilizzatore[23].

In questo contesto, secondo una parte della dottrina, il pericolo principale che deve essere scongiurato è quello di una imprudente confusione tra prova documentale e atto processuale[24]. Più precisamente, l'opera di creazione degli opportuni confini tra i diversi istituti, parte dalla considerazione per cui l'oggetto delle investigazioni informatiche in senso stretto, non è qualsiasi dato informatico in qualche maniera correlato con l'accertamento del reato. Più correttamente, i dati informatici che possono essere l'oggetto di *digital evidence* sono quelli dotati di una loro esistenza autonoma e indipendente rispetto al procedimento penale.

In quest'ottica le operazioni di ricerca di prove informatiche possono connotarsi per la loro staticità o per la loro dinamicità[25]. Nel primo caso, gli esperti estraggono elementi utili da un elaboratore; nel secondo, invece, vanno ad intercettare dati che circolano sulle reti. Nel primo caso, l'attività può essere condotta attraverso il sequestro e la perquisizione dello

[22] Sulla difficoltà di tracciare limiti precisi tra le intercettazioni "classiche" e il fenomeno regolato dall'art. 266 *bis* c.p.p. v., L. LUPÁRIA, Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, diretto da G. Spangher, *Modelli differenziati di accertamento*, Utet, Torino, 2011, vol. VII, t. I, p. 378, nt. 51.

[23] Così, G. DI PAOLO, *op. cit.*, p. 739.

[24] Ancora, G. DI PAOLO, *op. cit.*, p. 740.

[25] Si riprende una distinzione effettuata da G. ZICCARDI, *Aspetti informatico-giuridici della fonte di prova digitale*, in L. Lupària – G. Ziccardi, *op. cit.*, p. 49.

strumento elettronico ed ha come risultato l'ottenimento di un documento informatico[26]. Nel secondo caso, viceversa, l'autorità procedente opera, qualora ne sussistano i presupposti, secondo le modalità di cui all'art. 266 *bis* c.p.p.[27].

Oltre a quanto è stato esposto, vi è un'altra categorizzazione che può essere utile per permettere all'interprete di orientarsi nel vasto campo dei dati digitali rilevanti per il processo penale. Ci si riferisce alla distinzione di matrice anglo-americana tra *computer-derivated evidence* e *computer-generated evidence*[28]. Le prime, che potremmo definire prove di derivazione informatica, sono il corretto risultato delle attività di investigazione informatica in senso proprio: sono quei suoni, quelle immagini, quei *files* di testo o di *log* la cui esistenza precede l'attività inquirente[29]. Le seconde, invece, appellabili come prove a genesi informatica, hanno una forma più variegata. Queste, pur essendo accomunate dal fatto di essere dati informatici creati per il procedimento penale, assumono a seconda dei casi la veste di elementi probatori creati dal *computer*, oppure di atti processuali memorizzati su di un elaboratore o, infine, di dichiarazioni raccolte attraverso strumenti informatici.

[26] V., sul punto, F. ZACCHÈ, *La prova documentale*, Giuffrè, Milano, 2012, p. 34. In senso adesivo, S. DE FLAMMINEIS, *Le intercettazioni telematiche*, in *Dir. pen. proc.*, 2013, pp. 990 s.

[27] Non deve essere dimenticato come, l'attività di intercettazione di un flusso di dati possa anche essere compiuta attraverso forme atipiche, come il pedinamento virtuale. Sul tema, v. Cap. V., § 4.

[28] Cfr. L. LUPÁRIA, *La ricerca*, cit., p. 145.

[29] Il *file* di *log* è un *file* di testo generato automaticamente da un sistema operativo o da un *software*, il quale registra tutte le operazioni compiute tramite gli stessi. La dottrina, sulla base della distinzione tra traccia e documento, ha riconosciuto valenza di documento *ex* art. 243 c.p.p. anche ai *logfile*. Infatti, questi, pur creati automaticamente, sono frutto della volontà del programmatore che ha creato il *software* in modo da permettere che lo stesso tenesse traccia del suo stesso funzionamento. Questo rilievo vale a spiegare l'impossibilità di ricondurre i *files* di *log* alle categorie delle tracce; infatti, questi non solo non sono creati accidentalmente, ma, inoltre, hanno la piena capacità di rappresentare un fatto. Sul punto, ci si richiama a F. FOCARDI, *Art. 243*, in *Codice di procedura penale commentato*, a cura di A. Giarda, G. Spangher, Ipsoa, Milano, 4° ed., 2010, p. 2360; P. TONINI, *La prova documentale*, in P. Tonini – C. Conti, *Il diritto delle prove penali*, Giuffrè, Milano, 2012, p. 357, nt. 411. Per alcune notazioni di carattere tecnico sull'acquisizione, sull'analisi e sull'interpretazione di un *file* di *log*, v. A. GHIRARDINI – G. FAGGIOLI, *op.cit.*, pp. 367 ss.

Un primo esempio che potrebbe essere di aiuto nel chiarire in maniera più approfondita la distinzione proposta è quello del verbale redatto mediante *computer*[30]. In questo caso, lo strumento informatico viene utilizzato al fine di cristallizzare l'attività svolta dalle parti durante il compimento di un atto del procedimento. Sicuramente il risultato di questa operazione è, da un punto di vista tecnico-informatico, un documento informatico. Tuttavia, il *file* di testo prodotto dal verbalizzante, alla luce del motivo per cui è stato creato e per i soggetti che lo hanno redatto non può che essere qualificato come atto processuale. Infatti le modalità con cui viene effettuata la verbalizzazione non possono condurre alla modifica della natura dell'atto, trasformandolo in una prova digitale nel senso proprio del termine[31]. Identico discorso può essere compiuto per il caso in cui lo strumento digitale possa servire per documentare l'attività delle parti, come nel caso di registrazione audio/video di un interrogatorio. Anche in questa eventualità, non si è davanti ad una prova informatica. Infatti il dato digitale non viene estratto da un *device* elettronico connesso al fatto da accertare, ma, più correttamente, viene creato da questo in funzione del procedimento.

Vi è un'altra realtà che rischia di entrare in collisione con la *digital evidence*. Il riferimento corre a quei mezzi di ricerca della prova che, pur utilizzando strumenti elettronici,

[30] Per quanto riguarda le tecniche di redazione del verbale, il legislatore, anche al fine di dare attuazione ai princìpi di oralità e di massima semplificazione, ha preferito privilegiare l'utilizzo di strumenti tecnici per la redazione del verbale. Più in particolare, partendo dalla considerazione che in un processo dominato dall'oralità la verbalizzazione effettuata in caratteri comuni risultava inadeguata, l'art. 134 c.p.p. valorizza innanzitutto la verbalizzazione tramite stenografia e, successivamente, quella mediante altri mezzi meccanici. Tra questi rientra sicuramente anche l'utilizzo del *computer*. Come segnalato dalla dottrina, il legislatore non ha stabilito alcun rapporto gerarchico tra le varie forme di verbalizzazione ammesse dal codice di rito, lasciando quindi la possibilità di scelta dello strumento più opportuno al verbalizzante. Cfr. G. CONTI, *Forme di documentazione, forme di verbalizzazione e strumenti di documentazione: alcune precisazioni a margine di una sentenza della Corte costituzionale*, in *Cass. pen.*, 1991, II, p. 92. Più in generale sulla genesi dell'art. 134 c. p.p., v. M. BOUCHARD, *Art. 134*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. II, pp. 147 ss. In giurisprudenza, Cass. sez. V, 4 dicembre 2013, Gullo ed altro, in *C.e.d.* n. 258294 ha affermato la validità del verbale relativo ad operazioni di intercettazione anche se questo non viene successivamente stampato su di un supporto cartaceo.

[31] V. G. DI PAOLO, *op. cit.*, p. 741.

non hanno come obiettivo una realtà virtuale. Si sta alludendo alle intercettazioni, alle videoriprese e a tutti quei mezzi di ricerca della prova idonei a captare in presa diretta suoni, immagini o conversazioni[32]. In tutti questi casi, sarebbe errato fare riferimento alla *digital evidence*, in quanto il dato digitale che viene acquisito al processo risulta, ancora una volta, generato da un elaboratore su impulso delle stesse parti processuali. Siamo, anche in questo caso, nel campo delle *computer-generated evidence*.

Sempre avendo come obiettivo quello di delimitare correttamente il campo afferente alla *digital evidence*, è opportuno accennare ad altre due modalità di ingresso di dati informatici nel processo penale. La prima è rappresentata dall'eventualità in cui il sistema informatico rappresenti il mezzo dell'operazione probatoria: il riferimento è all'esame a distanza delle parti, grazie al quale entrano nel processo dati digitali di sicura valenza probatoria[33].

[32] L'inquadramento nelle categorie processuali delle videoriprese effettuate dalla polizia giudiziaria o da soggetti privati è stata oggetto di un corposo dibattito dottrinale e giurisprudenziale, al quale in questa sede, si può solo accennare. Innanzitutto, occorre distinguere le riprese effettuate in luoghi pubblici da quelle compiute all'interno del domicilio. Nel primo caso è necessario porre un'ulteriore distinzione tra le riprese compiute al di fuori del procedimento penale, per finalità ad esso estranee e quelle effettuate nel corso di un procedimento penale da parte della autorità giudiziaria. Le prime costituiranno dei documenti ammissibili *ex* art. 234 c.p.p.; viceversa, le seconde sono qualificate come prova atipica *ex* art. 189 c.p.p. Il discorso si complica, invece, per le riprese compiute all'interno del domicilio, in questo caso vi sarebbe un'altra distinzione da porre a seconda che le videoriprese abbiano ad oggetto comportamenti comunicativi ovvero mere condotte. Nel primo caso le videoriprese sono ricondotte alla disciplina delle intercettazioni e, quindi, possono essere utilizzabili solo se ottenute nel rispetto degli artt. 266 ss. c.p.p.; le seconde sono state oggetto di un corposo dibattito teso a definirne il perimetro della loro utilizzabilità in dibattimento. Un orientamento minoritario, pur rilevando un contrasto tra la registrazione di comportamenti non comunicativi all'interno del domicilio e l'art. 14 Cost., considerando la norma costituzionale inidonea ad essere direttamente applicata all'interno del procedimento penale, riteneva la prova così ottenuta utilizzabile. In senso opposto, la dottrina maggioritaria e la giurisprudenza, optano per l'inutilizzabilità della prova, pur se con percorsi argomentativi differenti. Alcuni hanno fatto riferimento alla teorica della prova incostituzionale, ossia di quella prova, definita da V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.*, 1973, p. 341 come quella «ottenut[a] attraverso modalità, metodi e comportamenti realizzati "in dispregio dei fondamentali diritti del cittadino"». Altri hanno ritenuto che i divieti di cui all'art. 191 c.p.p. potessero anche essere ricavati direttamente dalla Costituzione. Dal canto suo, Cass. sez. Un., 28 marzo 2006, Prisco, in *C.e.d. cass.* n. 234270, ha valorizzato l'art. 189 c.p.p. per farne discendere l'inammissibilità delle registrazioni effettuate nel domicilio. Infatti, non potrebbe essere ammesso come prova atipica un elemento probatorio che si forma in violazione della legge. Per una generale ricognizione del tema e gli opportuni riferimenti bibliografici si rimanda a C. CONTI, *Intercettazioni e inutilizzabilità: la giurisprudenza aspira al sistema*, in *Cass. pen.*, 2011, pp. 3638 ss.

[33] L'istituto è stato introdotto nel codice di procedura penale tramite il d.l. 8 giugno 1992, n. 306, convertito nella l. 7 agosto 1992, n. 356 il quale ha inserito nelle disposizioni di attuazione l'art. 147 *bis* disp. att. c.p.p. Successivamente il legislatore è intervenuto più volte sulla disciplina positiva dell'esame a distanza, da ultimo con la l. 13 agosto 2010, n. 36. Quella prevista dall'art. 147 *bis* disp. att. c.p.p. non è, tra l'altro, l'unica fattispecie di esame a

Tuttavia, nell'ipotesi in discorso i problemi che vengono posti sono radicalmente diversi da quelli afferenti al mondo della prova digitale. Infatti nell'esame a distanza il vero punto problematico è rappresentato dalla compatibilità dell'esame a distanza con il principio della formazione della prova nel contraddittorio e con il diritto dell'imputato di interrogare o far interrogare chi lo accusa[34]. Questioni relativamente irrilevanti per il mondo della prova informatica.

L'altra modalità di ingresso di dati digitali nel processo penale cui è opportuno accennare, è quella rappresentata dall'utilizzo del *computer* come strumento di simulazione del fatto di reato che deve essere accertato. In questo caso, mediante appositi *software* vengono ricreate le condizioni di spazio e di tempo in cui sarebbe accaduto l'illecito, al fine di testare la veridicità dell'ipotesi proposta da una delle parti. Questo potrebbe essere il campo dell'esperimento giudiziale, in cui il *computer* diventa il soggetto dell'attività probatoria e svolge la funzione di interpretare elementi fattuali già conosciuti dalle parti o dal giudice[35]. La prova creata attraverso l'elaboratore elettronico, in realtà, è a cavallo tra la prova informatica in senso stretto e quella creata dal *computer*. Per questa natura ibrida, alcuni in dottrina dubitano della sua riconducibilità al paradigma del citato esperimento giudiziale[36]. Seguendo questa corrente dottrinale, l'esperimento compiuto tramite un elaboratore dovrebbe

distanza prevista nel nostro ordinamento. Altre ipotesi sono previste dall'art. 205 *ter* disp. att. c.p.p. e dall'art. 7, co. 8 d.lgs. 6 settembre 2011, n. 159.

[34] Per una ricostruzione del dibattito dottrinale circa la compatibilità dell'esame a distanza con i princìpi di cui agli artt. 111, co. 4° Cost.; 6 § 3 lett. *d*) C.e.d.u. si rimanda a M. DANIELE, *La formazione digitale delle prove dichiarative. L'esame a distanza tra regole interne e diritto sovranazionale*, Giappichelli, Torino, 2012, pp. 13 ss.

[35] L'istituto, regolato dagli artt. 218, 219 c.p.p., consente alle parti di chiedere l'organizzazione di un esperimento su di un fatto certo per accertare come questo possa essere accaduto. Come segnalato da F. CORDERO, *Procedura penale*, Giuffrè, Milano, 9° ed., 2012, p. 780 gli esperimenti più utili sono quelli di carattere negativo tramite questi, infatti, è possibile smentire tesi insostenibili. Viceversa, un esperimento che accerti la possibilità che un certo fatto sia accaduto secondo certe modalità, non permette di giungere alla conclusione che quella sia l'unica modalità in cui può rappresentarsi l'accadimento.

[36] G. DI PAOLO, *op. cit.*, pp. 742 s.

essere ricompreso nelle prove atipiche *ex* art. 189 c.p.p. e ammesso come tale. Ciò per due motivi concorrenti. In primo luogo, la simulazione computerizzata dell'evento non risulta disciplinata da nessuna norma processuale; in secondo luogo, questa costituirebbe un esempio di quella *novel science* per la quale autorevole dottrina ha suggerito l'applicazione in via analogica dell'art. 189 c.p.p. al fine di garantire un pieno sindacato del giudice in ordine all'ammissibilità della prova[37].

Volendo dare una prima definizione di fonte di prova digitale, si può affermare come questa sia costituita da tutti quei dati informatici formati esternamente e per finalità indipendenti dal processo penale, che risultino pertinenti per la dimostrazione della verità o della falsità dell'enunciato accusatorio contenuto nell'atto di imputazione formulato dal pubblico ministero. All'interno di questa categoria è possibile effettuare una prima distinzione a seconda dell'origine dei dati informatici. Infatti, da una parte vi sono quelle evidenze digitali contenute stabilmente su di un *device* elettronico, sia questo un *computer*, un *tablet* o uno *smartphone* e, dall'altra, vi sono tutte quelle informazioni circolanti in una rete, come nel caso di *Internet*, che vengono attivamente captate dagli inquirenti. Le prime possono essere qualificate come documenti informatici, mentre le seconde come flusso di dati informatici.

[37] Ci si riferisce alla tesi sostenuta da O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005, pp. 102 ss. Per una ricognizione più generale del dibattito generale in merito all'ammissione della prova scientifica nuova si rimanda alle considerazioni svolte nel Cap. I.

3. La *digital evidence* come documento informatico

Alla luce della distinzione effettuata nel paragrafo precedente, si può affermare come il tema della prova informatica sia, almeno in parte, legato a doppio filo con quello del documento informatico. Infatti, qualsiasi operazione di estrazione di *digital evidence* da un dispositivo elettronico si risolve sempre nell'acquisizione di un documento di carattere informatico[38]. Si pone, pertanto, la questione circa la definizione giuridica da assegnare a tale espressione.

Il tema del documento informatico è stato affrontato sotto diversi profili da vari Autori, ciascuno dei quali ne ha sottolineato un aspetto particolare funzionale al proprio campo di ricerca.

Dal canto suo, il legislatore ha mostrato più di un'incertezza nella delimitazione del concetto di documento informatico. Questi, infatti, ne ha ripetutamente riformulato la definizione.

Da un punto di vista cronologico, la prima definizione di documento informatico risulta essere quella introdotta con la l. 23 dicembre 1993, n. 547, attraverso la previsione di cui all'art. 491 *bis* c.p.[39]. Nel secondo periodo di tale disposizione si precisava che per documento informatico dovesse intendersi «qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli». Il legislatore, animato dalla volontà di estendere le norme che reprimono i falsi docu-

[38] Cfr., F. ZACCHÉ, *op. cit.*, p. 34. In giurisprudenza, v. Cass. sez. III, 5 luglio 2012, Lafuenti, in *C.e.d. cass.* n. 253573.

[39] L'intervento legislativo è stato posto in essere sulla base della Raccomandazione 13 settembre 1989, R (89) 9 del Consiglio d'Europa in tema di criminalità informatica. Per maggiori dettagli sulla raccomandazione si rimanda a C. PECORELLA, *Diritto penale dell'informatica*, Cedam, Padova, 2006, pp. 7 ss.

mentali anche ai falsi informatici, aveva coniato una definizione alquanto singolare di documento informatico[40]. Infatti al centro della stessa veniva posto il supporto contenente le informazioni. Nella relazione al disegno di legge si affermava che «si è ritenuto [...] di attribuire la natura di documento informatico ai «supporti» – di qualunque specie essi siano – contenenti dati, informazioni o programmi». La logica sottesa a tale opzione normativa era stata quella di evitare di scardinare la sistematica del codice penale in tema di falsità dei documenti[41]. Infatti, affermavano i sostenitori della disposizione, se si tutela il supporto allora si protegge anche ciò che è in esso contenuto[42]. La scelta del legislatore, criticabile sotto certi aspetti, si riallacciava ad un orientamento dottrinale diffuso principalmente nella letteratura civilistica. Secondo questa impostazione, il documento sarebbe un *opus* risultante dal lavoro dell'uomo[43]. Più precisamente, il documento sarebbe un oggetto della realtà sensibile sul quale sono impressi dei segni o direttamente dall'uomo o da una macchina per il tramite di quest'ultimo. I segni presenti sul documento svolgerebbero la funzione di aiutare il lettore a rappresentarsi nella propria mente il fatto descritto tramite l'oggetto[44]. Per queste ragioni, il

[40] Per un'analisi della fattispecie introdotta, v. C. PARODI, *Il documento informatico nel sistema normativo penale*, in *Dir. pen. proc.*, 1998, p. 369; L. PICOTTI, *Commento all'art. 3 l. 23 dicembre 1993, n. 547*, in *Leg. pen.*, 1996, pp. 62 ss. Più in generale sul tema della tutela apprestata al documento informatico da parte dell'ordinamento penale, v. P. TRONCONE, *La tutela penale del documento dematerializzato tra vicende normative e nuove aspirazioni sistematiche*, in *Riv. pen.*, 2008, pp. 1277 ss.

[41] M. PETRONE, *Le recenti modifiche del codice penale in tema di documento informatico: problemi e prospettive*, in *Dir. Inf.* 1995, p. 263, osservava come accettando l'idea del dato informatico come pensiero sganciato dalla sua materialità, si renderebbe necessario modificare tutte le fattispecie di falso documentale. Infatti, i concetti di falso materiale, falso ideologico, falso per soppressione hanno valore solo se riferiti al documento come *res*. La diversa opzione interpretativa avrebbe comportato o l'inapplicabilità delle disposizioni sul falso oppure la loro applicazione in via analogica. Soluzioni che parevano parimenti inaccettabili per l'Autore.

[42] V., M. PETRONE, *op. cit.*, p. 263. Nella medesima direzione, C. SARZANA DI S. IPPOLITO, *Informatica e diritto penale*, Giuffrè, Milano, 1994, pp. 209 s.

[43] Cfr. N. IRTI, *Norme e fatti. Saggi di teoria generale del diritto*, Giuffrè, Milano, 1984, p. 247.

[44] Ancora, N. IRTI, *op. cit.*, p. 257.

documento sarebbe costituito da un oggetto percepibile dal quale è dato pronunciare il giudizio di esistenza di un fatto che sia sussumibile sotto un tipo normativo[45].

La definizione di documento informatico fatta propria dalla l. n. 547/1993 è rimasta in vigore nell'ordinamento italiano fino al 2008, quando la l. 18 marzo 2008, n. 48, tramite la quale è stata ratificata la convenzione di Budapest sul *cybercrime*, ha disposto la modifica dell'art. 491 *bis* c.p.[46].

Guardando al tema del documento informatico da un'altra prospettiva, il legislatore ne ha fornito un'altra e diversa definizione. Infatti il d.lgs. 7 marzo 2005, n. 82 – ossia il codice dell'amministrazione digitale – lo ha definito come «la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti[47]». In questo caso, la prospettiva accolta sarebbe quella di un'autorevole dottrina, la quale ha studiato il fenomeno della prova documentale in relazione al processo civile. Questi, infatti, descrive il documento tradizionale come un oggetto in grado di rappresentare qualcos'altro. Sarebbe intrinseca ad alcune *res* la capacità di evocare sensazioni analoghe ad altri oggetti, costituendone quindi un «equivalente sensibile[48]». Questo potere di raffigurazione sarebbe implicito al contenuto rappresentativo di ogni documento. Secondo tale prospettazione, tre sarebbero gli elementi costituitivi della prova documentale: la materia, il mezzo e il contenuto. La prima è composta da ciò su cui vengono posti

[45] N. IRTI, *op. cit.*, p. 260.

[46] Per una generale ricognizione degli interventi effettuati tramite la l. 18 marzo 2008, n. 48 v., per tutti, L. PICOTTI – L. LUPÁRIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa*, in *Dir. pen. proc.*, 2008, pp. 696 ss.

[47] Per una panoramica sul tema del documento informatico nelle pubbliche amministrazioni si rimanda a F. FERRARI, *Il codice dell'amministrazione digitale e le norme dedicate al documento informatico*, in *Riv. dir. proc.*, 2007, p. 415.

[48] Cfr. F. CARNELUTTI, *Documento (teoria moderna)*, in *Novissimo dig. it.*, vol. VI, p. 86.

dall'uomo i segni rappresentativi. Il secondo dagli strumenti utilizzati per descrivere un determinato fatto. Il terzo è, appunto, ciò che il documento descrive e quindi, ciò che questo rappresenta[49].

Attualmente, la definizione appena accennata rimane quella accettata dal nostro ordinamento, poiché la l. n. 48/2008 non ha modificato le disposizioni del codice dell'amministrazione digitale sul tema. Tuttavia, quest'ultima risulta essere, almeno in parte, ai fini di cui innanzi, poco utile. Ciò in quanto, la norma del codice dell'amministrazione digitale sarebbe di difficile armonizzazione con la normativa processuale penale.

Infatti l'art. 234 c.p.p., seppur ispirato all'idea di documento come oggetto idoneo a rappresentare qualcosa, accoglie una nozione di documento leggermente diversa[50]. La disposizione afferma 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». Ad una prima lettura, in linea con l'opzione ermeneutica appena sopra accennata, sembrerebbe che la fotografia, la cinematografia e la scrittura costituiscano dei mezzi di rappresentazione di un fatto. In dottrina vi è chi ha sottolineato l'imprecisione della formula adottata dal legislatore nell'art. 234 c.p.p.[51]. Infatti i mezzi di rappresentazione sono, più propriamente, le parole o le immagini. Invece, la fotografia o la scrittura costituirebbero

[49] V., ancora F. CARNELUTTI, *op. cit.*, p. 86.

[50] La dottrina processualpenalista ha elaborato varie teorie circa la definizione di documento rilevante per il processo penale. Oltre quella accolta nel testo, merita di essere segnalata quella di G. UBERTIS, *Documenti e oralità*, in *Evoluzione e riforma del diritto e della procedura penale, 1945-1990: studi in onore di Giuliano Vassalli*, a cura di M.C. Bassiouni – A.R. Latagliata – A.M. Stile, Giuffrè, Milano, 1991, vol. II, pp. 301 s., il quale definisce il documento come una «entità materiale intenzionalmente rappresentativa di altro, giuridicamente rilevante, rispetto alla propria consistenza sensibile».

[51] In tal senso, P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, pp. 402 s.

mezzi di incorporazione della parola o dell'immagine su di un certo supporto fisico. Il retroterra culturale di una tale opzione ermeneutica è rappresentato da alcune ricostruzioni dogmatiche proprie della scienza penalistica sviluppatesi in tema di falso documentale[52].

L'idea dell'incorporamento dovrebbe fungere da guida all'interprete per la corretta definizione del documento informatico. Questa, infatti, dovrebbe essere descritto come un oggetto nel quale sono incorporati, con modalità informatiche, dei fatti[53].

La definizione appena fornita sembrerebbe essere quella implicitamente accettata dal legislatore del 2008, allorché è intervenuto sul codice di procedura penale per dare attuazione alla convenzione di Budapest sul *cybercrime*[54]. L'idea principale sottesa alle modifiche del codice di rito penale è stata quella di garantire in ogni caso l'immodificabilità del dato informatico raccolto. Questa necessità, prosegue la dottrina in discorso, può essere compresa alla luce della particolarità del metodo di incorporamento. Quello informatico, infatti, è un metodo di incorporamento capace di creare documenti dematerializzati[55]. La possibilità di convertire parole, suoni o immagini in impulsi elettronici comporta, come già accennato, il potere di accedere a tali informazioni in maniera indipendente rispetto al supporto sul quale esse sono contenute. Questo significa che per accedere ad una certa sequenza di *bit* non è necessario avere in custodia la *res* sulla quale queste sono state memorizzate per la prima

[52] V., sul punto, A. MALINVERNI, *Teoria del falso documentale*, Giuffrè, Milano, 1958, p. 69

[53] Cfr. P. TONINI, *Il documento informatico: problematiche civilistiche e penalistiche a confronto*, in *Corr. giur.*, 2012, p. 434.

[54] Così, P. TONINI, *Il documento*, cit., p. 435.

[55] Nonostante si faccia sempre più riferimento al documento informatico come ad un documento immateriale, alcuni Autori hanno ritenuto più corretto definire lo stesso come documento dematerializzato. Infatti, il documento informatico ha una sua base fisica, costituita dagli impulsi elettrici, magnetici o luminosi presenti sul supporto sul quale lo stesso è memorizzato. Viceversa, ponendo l'accento sulla dematerialità del documento si pone in risalto quella che è la caratteristica fondamentale di un tale atto, ossia il fatto che questo, pur esistendo indipendentemente rispetto al supporto su cui è memorizzato, necessiti lo stesso di un *hard disk*, *pendrive*, o altro mezzo per esistere. Cfr. P. TONINI, *Il documento informatico*, cit., p. 434, il quale si riallaccia alle riflessioni di F. ALCARO, *Riflessioni "vecchie" e "nuove" in tema di beni immateriali. Il diritto d'autore nell'era digitale*, in *Rass. dir. civ.*, 2006, pp. 950 s.

volta. Come rilevato, il contenitore è «necessario per fissare *una tantum* il contenuto[56]». Conseguenza di tale metodo di incorporamento è lo scarso livello di stabilità tra il supporto materiale e ciò che è registrato su di esso. Mentre nel caso dei documenti tradizionali, il contenuto rappresentativo è fissato in maniera definitiva sullo stesso; nei documenti informatici, questo può essere facilmente copiato su un altro dispositivo. Il principale problema connesso a tale proprietà è quello di garantire la genuinità delle informazioni presenti sul documento. Infatti nel documento tradizionale eventuali manomissioni possono essere compiute solo attraverso condotte che vanno a modificare fisicamente l'oggetto della rappresentazione in maniera irreversibile. Per questo motivo, una falsificazione dello stesso può essere relativamente semplice da rilevare. Il documento informatico, viceversa, proprio a causa della facilità con cui può essere spostato da un supporto ad un altro può essere modificato senza apparire, almeno ad una prima analisi, manipolato. Questa differenza rende chiara la scelta del legislatore di differenziare nettamente il procedimento di copia dei documenti informatici rispetto a quelli tradizionali[57]. Per i primi, da un lato, si ammette all'art. 234, co. 2° c.p.p. di acquisirne una copia qualora l'originale sia stato distrutto e, dall'altro, si prevede la possibilità, *ex* art. 258 c.p.p., per l'autorità sequestrante di effettuare copia dei documenti sequestrati per poi restituire gli originali al soggetto che ha subìto il sequestro. In entrambi i casi viene lasciata ampia libertà agli inquirenti circa le modalità di effettuazione di tali operazioni, sul presupposto della semplicità dell'operazione di copiatura. Per i secondi, viceversa, alla luce della fragilità del dato informatico, viene imposto agli inquirenti la necessità di scegliere metodi di copiatura che non solo possano garantire la conformità tra la copia e l'originale, ma

[56] In tal senso E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, p. 1525.

[57] Cfr. E. LORENZETTO, *op. cit.*, p. 1526.

anche che i dati originali non siano modificati in alcun modo attraverso l'operazione di copiatura.

Alla luce delle motivazioni esposte si ritiene pertanto di aderire a quella opinione che qualifica il documento informatico come una *res* dematerializzata immessa su di un supporto fisico attraverso un metodo di incorporamento digitale.

4. La *digital evidence* come flusso di dati

Come è stato precedentemente evidenziato, la *digital evidence* si può presentare anche sotto una diversa forma: quella di un flusso di dati. In questa situazione, l'apprensione della fonte di prova digitale avviene attraverso modalità definite dinamiche.

La principale norma che viene in rilievo allorché si faccia riferimento alla *digital evidence* come flusso di dati è l'art. 266 *bis* c.p.p. La disposizione è stata inserita nel codice di rito penale dalla già citata l. n. 547/1993, al fine di fornire adeguati strumenti di contrasto alla criminalità informatica. L'opera del legislatore si è sviluppata ammettendo la possibilità di poter disporre intercettazioni di comunicazioni informatiche o telematiche sia per i reati previsti dall'art. 266 c.p.p. sia per tutti i reati commessi attraverso «l'impiego di tecnologie informatiche o telematiche».

L'introduzione di una disposizione *ad hoc* per conferire il potere di disporre l'intercettazione di un flusso di dati tra sistemi informatici è stata criticata da alcuni[58]. Infatti l'art. 266 c.p.p., contenendo una clausola di carattere generale ideata proprio per permettere un automatico aggiornamento della normativa codicistica alle nuove tecnologie, già affidava alla magistratura la possibilità di poter richiedere l'effettuazione di intercettazioni di stampo informatico[59]. Non solo: sarebbe, secondo altri, criticabile anche la scelta compiuta dal legi-

[58] Cfr. G. FUMU, *Art. 266* bis, in *Commento al codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1997, agg. III, p. 132. Sulla stessa linea, v. A. CAMON, *Le intercettazioni nel processo penale*, Giuffrè, Milano, 1996, pp. 11 ss., il quale, inoltre, sottolinea come la clausola aperta scelta dal legislatore del 1988 abbia il pregio di evitare qualsiasi tentazione di ricondurre eventuali nuove forme di intercettazioni al concetto di atipicità probatoria. In tal modo, prosegue l'Autore, si offre una tutela più forte circa l'effettiva segretezza delle comunicazioni.

[59] Cfr., ancora, A. CAMON, *op. cit.*, p. 13, che evidenzia come l'introduzione dell'art. 266 *bis* c.p.p. rischi di scardinare il sistema delineato dal legislatore. Infatti, se per intercettare forme di comunicazione diverse da quella telefonica fosse sempre necessario l'intervento della legge ordinaria, allora sarebbe necessaria la predisposizione di una norma *ad hoc* per rendere ammissibile l'intercettazione di un fax.

slatore di ammettere l'utilizzo di un peculiare strumento di indagine particolarmente invasivo, allorché gli illeciti siano compiuti attraverso apparecchiature informatiche. In questa eventualità si assisterebbe, infatti, ad una disparità di trattamento tra indagati che, pur essendo sottoposti alle indagini per il medesimo reato, potrebbero subire una maggiore compressione dei propri diritti fondamentali sulla base del mezzo utilizzato per compiere l'illecito[60].

Nonostante l'espressa previsione del potere di disporre un'intercettazione informatica o telematica, il legislatore non ha comunque fornito alcuna definizione di tale istituto. Soccorre a tal proposito la considerazione per cui tra l'art. 266 c.p.p. e l'art. 266 *bis* c.p.p. vi sarebbe un rapporto di genere a specie. Infatti il secondo non sarebbe altro che una particolare forma di intercettazione di comunicazioni. Da ciò ne discende la possibilità di definire il fenomeno delle intercettazioni telematiche, alla luce delle intercettazioni "classiche". Secondo la dottrina maggioritaria, gli elementi costitutivi di un'intercettazione sono tre: la captazione di una conversazione riservata, la terzietà del soggetto che ascolta, la contemporaneità tra ascolto e conversazione[61]. Lo strumento previsto dall'art. 266 *bis* c.p.p. non fa eccezione. In senso generale, si è, quindi, in presenza di una intercettazione informatica o tele-

[60] In tal senso, L. UGOCCIONI, *Commento all'art. 11 l. 23 dicembre 1993, n. 547*, in *Leg. pen.*, 1996, pp. 142 s. Sulla stessa linea si pone anche L. LUPÁRIA, *Le investigazioni informatiche nell'ordinamento italiano*, in L. Lupária – G. Ziccardi, *op. cit.*, pp. 162 s., il quale, tuttavia, sottolinea una parte delle criticità teoriche sottese alla scelta del legislatore. Infatti, alcuni degli strumenti utilizzati dalla polizia giudiziaria per effettuare un'intercettazione telematica captano contemporaneamente anche conversazioni telefoniche. Questo permetterebbe, in via astratta, di intercettare conversazioni telefoniche anche per reati non previsti dall'art. 266 c.p.p. Tale possibilità, prosegue l'Autore, dovrebbe essere esclusa nella pratica grazie all'utilizzo di appositi apparati che rendono inascoltabile l'eventuale traffico telefonico intercettato al di fuori dei limiti previsti dalla legge.

[61] Cfr. G. FUMU, *Art. 266*, in *Commento*, cit., p. 774. La definizione proposta permette di fare chiarezza in alcune situazioni particolari, come, per esempio, la registrazione della telefonata da parte di uno dei due conversanti. Per alcuni spunti in tal senso, v. A. CAMON, *op. cit.*, pp. 16 ss.

matica, tutte le volte in cui un soggetto terzo capti una conversazione riservata, non necessariamente vocale, tra almeno due sistemi informatici o telematici[62]. Ammessa questa ampia definizione, sono necessarie alcune precisazioni. La prima ha ad oggetto la fonte del flusso di dati. Infatti l'art. 266 *bis* c.p.p. non si occupa di qualsiasi scambio di dati tra sistemi informatici, ma solo di quel flusso di comunicazioni che sia il frutto di un'attività comunicativa umana[63]. Inoltre, è fondamentale che la captazione dei dati avvenga in tempo reale, ossia durante la loro trasmissione. Infatti questo requisito vale a differenziare l'istituto dell'intercettazione informatica dal sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni regolato dall'art. 254 *bis* c.p.p.[64]

La disposizione citata non regola tutte le fattispecie di ingresso di flussi di dati informatici all'interno del processo penale, tuttavia gli altri strumenti che consentono una tale captazione sono da ritenersi esclusi dal perimetro applicativo di tale norma. Questi, infatti, come si avrà modo di osservare più avanti, sono da ricondurre al momento, allo schema della prova c.d. atipica[65].

[62] Da un punto di vista tecnico, la differenza tra sistema informatico e sistema telematico è data dalle modalità attraverso cui gli elaboratori si scambiano i dati. Infatti, solo nel secondo caso la trasmissione dei dati avviene grazie alla rete telefonica o, in alcuni casi, per il tramite di reti satellitari. Per un maggiore approfondimento, si rimanda alle considerazioni di G. BUONOMO, *Metodologia e disciplina delle indagini informatiche*, in R. Borruso – G. Buonomo – G. Corasaniti – G. D'Aietti, *Profili penali dell'informatica*, Giuffrè, Milano, 1994, pp. 148 ss.

[63] La precisazione aiuta ad inquadrare meglio fenomeni particolari come quello, che verrà analizzato più avanti, dell'intercettazione di un segnale g.p.s. inviato, ad esempio, da un navigatore satellitare. Cfr., G. DI PAOLO, *op. cit.*, p. 744.

[64] L'art. 254 *bis* c.p.p. è stato introdotto dal legislatore attraverso la l. n. 48/2008, con la quale è stata ratificata la Convenzione di Budapest sul *cybercrime*. I soggetti destinatari della disposizione sono i fornitori di connettività, ai quali l'autorità giudiziaria può richiedere i dati da questi detenuti per le finalità proprie del servizio offerto. Nel disegnare tale possibilità, il legislatore ha cercato un punto di equilibrio tra le esigenze investigative e quelle proprie dei *service providers*. A tal fine, l'art. 254 *bis* c.p.p. prevede la possibilità di fornire alla magistratura copia dei dati richiesti, tutte le volte in cui la fornitura di tali dati in originale potrebbe compromettere la corretta erogazione del servizio. Sulla linea di demarcazione tra l'art. 266 *bis* c.p.p. e l'art. 254 *bis* c.p.p. si avrà modo di ritornare nel Cap. IV, § 5.

[65] In tema di prova atipica si richiamano le considerazioni di cui al Cap. I, § 2.

Per quanto attiene alle prove digitali di carattere dinamico, queste possono, quindi, essere definite come tutti quei dati sia comunicativi sia esterni alla comunicazione che circolano tra le reti di strumenti elettronici e che, acquisiti in tempo reale, possono dirsi rilevanti per il procedimento penale.

Capitolo III

Prova informatica e diritti fondamentali della persona

SOMMARIO: 1. Diritti fondamentali e digital forensics*: un'introduzione – 2. Il diritto alla riservatezza in àmbito nazionale ed europeo – 3. (segue): dalla tutela della vita privata nella Convenzione europea dei diritti dell'uomo alla delimitazione della riservatezza informatica – 4. L'evoluzione del concetto di domicilio accettato nella Costituzione e nella Convenzione europea dei diritti dell'uomo – 5. Le garanzie di libertà e segretezza delle comunicazioni*

1. Diritti fondamentali e *digital forensics*: un'introduzione

Nel precedente capitolo, si è avuto modo di offrire una prima delimitazione delle attività che possono essere svolte allorché si presenti la necessità di acquisire elementi probatori di carattere informatico. Ad una prima riflessione, emerge, immediatamente, l'idea per cui tali atti non possono dirsi indifferenti per l'individuo che li subisce, nel senso che, qualsiasi operazione di raccolta e repertamento di dati informatici va a comprimere alcuni diritti fondamentali del singolo. Tale limitazione, connaturata all'attività di raccolta di elementi probatori durante la fase investigativa e non solo, deriva, principalmente, dalla già ricordata espansione dell'informatica nella vita quotidiana[1].

[1] Si richiamano le considerazioni svolte nel Cap. II, § 1.

Volendo proporre una prima e sommaria elencazione delle posizioni giuridiche soggettive che vengono in rilievo, può evidenziarsi come queste siano da individuare principalmente nei diritti di riservatezza, inviolabilità del domicilio e libertà e segretezza delle comunicazioni. Sul punto, deve, in prima battuta, essere sottolineato come questa triade possa essere più plasticamente rappresentata facendo riferimento ad un triangolo al cui vertice più alto vi sia la riservatezza e che abbia alla base l'inviolabilità del domicilio e la garanzia circa la libertà e segretezza delle comunicazioni. Infatti, come ha avuto modo di osservare anche la Corte costituzionale in una celebre pronuncia in tema di legittimità di videoriprese all'interno del domicilio, i beni giuridici cui fanno riferimento gli artt. 14 e 15 Cost. costituiscono «espressioni salienti di un più ampio diritto alla riservatezza della persona[2]».

Al di là del contenuto dei diritti citati, tema che sarà trattato nei prossimi paragrafi, deve essere rilevato come la tutela offerta alla riservatezza, al domicilio e alla segretezza e alla libertà delle comunicazioni si caratterizza per essere attuata attraverso un sistema multilivello. Infatti i diritti in discorso non sono nominati soltanto all'interno della nostra Costituzione, ma ricevono espressa protezione anche dalla Convenzione europea per la salvaguardia dei diritti dell'uomo, dalla Carta di Nizza e, più in generale dal diritto dell'Unione europea. In questo contesto, il punto di partenza di questa, necessariamente sommaria, trattazione circa i diritti fondamentali rilevanti per la *digital forensics* non può che essere rappresentato da alcune considerazioni di carattere generale riguardanti il grado da assegnare a queste fonti nell'ordinamento italiano.

[2] Cfr. Corte cost., 24 aprile 2002, n. 135, in *Giur. cost.*, 2002, pp. 1062 ss. con nota di A. PACE, *Le videoregistrazioni «ambientali» tra gli artt. 14 e 15 Cost.*

Tralasciando il valore da attribuire al diritto dell'Unione europea nel nostro ordinamento, in quanto la questione, dopo numerosi dibatti che hanno impegnato anche la giurisprudenza costituzionale può dirsi in gran parte risolta anche alla luce della modifica all'art. 117 Cost., il quale parrebbe aver recepito il principio di prevalenza del diritto dell'Unione europea[3]; risulta più opportuno concentrare l'attenzione sul valore da attribuire alla C.e.d.u. e alla Carta di Nizza.

Primariamente, è necessario ribadire la diversità delle due carte dei diritti alla luce delle istituzioni che le hanno predisposte ed emanate. La Convenzione europea per la salvaguardia dei diritti fondamentali è stata emanata dal Consiglio d'Europa, un'organizzazione internazionale nata subito dopo la fine della seconda guerra mondiale al fine di incentivare la tutela dei diritti umani in Europa. Di questa organizzazione fanno parte al momento 47 Stati, motivo per cui è stata definita da alcuni la grande Europa[4]. Viceversa, la Carta di Nizza è espressione della volontà dell'Unione europea, ossia la piccola Europa, di offrire una tutela dei diritti umani all'interno dei Paesi membri della stessa. La conseguenza principale di questa distinzione, come si avrà modo di vedere in seguito, è data dal valore che queste carte dei diritti hanno nell'ordinamento italiano e, soprattutto, dal metodo di risoluzione di eventuali antinomie tra la legge ordinaria e uno di questi due trattati.

Sul valore giuridico da assegnare alla C.e.d.u., la dottrina costituzionalistica e la stessa Corte costituzionale hanno discusso a lungo[5]. Non essendo opportuno ripercorrere tutte le

[3] Sul valore generale da attribuire a tale intervento legislativo per quanto riguarda la gerarchia delle fonti internazionali nel nostro ordinamento, v. *infra* nel testo. Il citato principio di primazia del diritto dell'Unione europeo è stato accettato da Corte cost., 8 giugno 1984, n. 170, in *Giur. cost.*, 1984, pp. 1098 ss.

[4] Ci si riferisce alla classificazione proposta da F. VIGANÒ, *Fonti europee e ordinamento italiano*, in *Europa e diritto penale*, a cura di F. Viganò – O. Mazza, Ipsoa, Milano, 2011, pp. 4 s.

[5] I rapporti tra il nostro ordinamento e la C.e.d.u. possono essere suddivisi in tre macro periodi. Il primo, comprendente un arco temporale che va dalla ratifica della stessa fino ai primi anni '90 del '900, vede la Convenzione equiparata alla legge ordinaria. Ciò in ragione del fatto che l'ingresso della C.e.d.u. nel nostro ordinamento av-

discussioni sul punto, ci si limiterà a dar conto del risultato cui è giunto questo lungo dibattitto grazie al fondamentale contributo fornito dalla giurisprudenza costituzionale. Infatti la Corte costituzionale in due sentenze, definite dalla dottrina "gemelle", ha delineato in maniera esaustiva il valore da assegnare nella gerarchia delle fonti alla C.e.d.u.[6]. La soluzione prescelta è stata quella di riconoscere alla stessa il valore di norma interposta, ossia di norma che pur non essendo di rango costituzionale, può tuttavia, integrare un precetto della Costituzione, permettendo al giudice delle leggi di poter sindacare la compatibilità tra una legge ordinaria e la C.e.d.u.

La strada che conduce a tale soluzione prende le mosse dall'interpretazione dell'art. 117, co. 1° Cost., il quale, nel testo risultante a seguito della modifica effettuata attravero la l. cost. 18 ottobre 2001, n. 3, stabilisce che «la potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali». Tra le varie interpretazioni possibili di tale disposizione, la Corte costituzionale ha preferito quella che permettesse di adeguare il nostro ordinamento agli obblighi derivanti dalla ratifica della C.e.d.u.[7]. Infatti i giudici costituzionali

viene tramite legge ordinaria, ossia con la l. 4 agosto 1955, n. 848. Successivamente, sia la giurisprudenza costituzionale sia la dottrina, a causa del contenuto valoriale della Convenzione, iniziano a cercare una copertura costituzionale che valga a differenziare la C.e.d.u. dalla legge ordinaria. Gli agganci costituzionali sono di volta in volta ricercati prima nell'art. 10 Cost., poi nell'art 11, co. 2° Cost. e, infine, nell'art. 2 Cost. Tuttavia, nessuna delle teorie proposte pare pienamente convincente. L'ultimo periodo è quello successivo alle c.d. sentenze gemelle della Corte costituzionale, di cui si darà conto più avanti nel testo, nel quale la Convenzione europea per i diritti dell'uomo va ad integrare l'art. 117, co. 1° Cost. diventando una norma interposta. Per un'esauriente ricostruzione delle posizioni giurisprudenziali e dottrinali sul punto, si rimanda a M. CARTABIA, *La convenzione europea dei diritti dell'uomo e l'ordinamento italiano*, in *Giurisprudenza europea e processo penale italiano. Nuovi scenari dopo il «caso Dorigo» e gli interventi della Corte costituzionale*, a cura di A. Balsamo – R. E. Kostoris, Giappichelli, Torino, 2008, pp. 37 ss.

[6] Ci si riferisce a Corte cost., 24 ottobre 2007, n. 348 in *Giur. cost.*, 2007, pp. 3475 ss. e Corte cost., 24 ottobre 2007, n. 349 in *Giur. cost.*, 2007, pp. 3535, con note di M. CARTABIA, *Le sentenze «gemelle»: diritti fondamentali, fonti, giudici*; A. GUAZZAROTTI, *La Corte e la CEDU: il problematico confronto di* standard *di tutela alla luce dell'art. 117, comma 1 Cost.*; V. SCIARABBA, *Nuovi punti fermi (e questioni aperte) nei rapporti tra fonti e corti nazionali ed internazionali.*

[7] Le interpretazioni dell'art. 117, co. 1° Cost. sono raggruppabili in tre filoni. Secondo un primo orientamento, il nuovo testo della disposizione, alla luce della sua collocazione sistematica e in relazione ai lavori preparatori, non sarebbe in grado di innovare una materia così complessa come quella dei rapporti tra Stato italiano e fonti internazionali. Sul versante opposto, vi era chi riteneva che con questa modifica il legislatore costituzionale avesse

hanno ritenuto come la limitazione della potestà legislativa derivante dal rispetto degli obblighi internazionali non potesse essere letta come operante solamente nei rapporti tra Stato e Regioni, nonostante l'articolo in commento si trovi nel Titolo V, riservato, appunto, a tale tema.

La Corte prosegue nella sua argomentazione rilevando come l'art. 117, co. 1° Cost. sia una disposizione che, per poter spiegare i suoi effetti tipici, deve in qualche modo essere riempita di contenuto. Infatti il vincolo che è imposto al legislatore ordinario acquista concretezza solo se si individuano i contenuti degli obblighi internazionali cui si è sottoposta l'Italia.

Tra gli obblighi internazionali idonei a integrare il parametro costituzionale, la Corte riconosce preminente importanza alla C.e.d.u., la quale, in ragione anche della creazione di un organo apposito deputato all'interpretazione della stessa, comporta l'obbligo per il legislatore italiano di adeguare la normativa interna alle norme della Convenzione, così come interpretate dai giudici della Corte e.d.u. Tale forma di riconoscimento non comporta, tuttavia, la costituzionalizzazione della Convenzione europea dei diritti dell'uomo, la quale, andando ad integrare il parametro di costituzionalità, si trova a dover rispettare la Costituzione stessa. Ciò per evitare, proseguono i giudici, che la Corte si trovi a dover dichiarare l'incostituzionalità di una disposizione contraria ad una fonte sub-costituzionale, a sua volta contra-

inteso creare una clausola di adattamento automatica ai trattati internazionali. Tra questi due estremi, si inserisce una lettura mediana, la quale ritiene che il tratto innovativo della riforma sia da ricercare nella nuova forza di resistenza passiva dei trattati internazionali nei confronti delle leggi ordinarie, le quali dovranno essere emanate nel rispetto degli obblighi internazionali. Per una ricostruzione del dibattito sommariamente descritto, v. ancora M. CARTABIA, *La convenzione europea*, cit., pp. 46 ss.

ria alla Costituzione stessa. Per cui, compito della Corte è sempre quello di verificare la compatibilità costituzionale del parametro interposto invocato dal giudice *a quo*, dichiarando, nel caso, l'inidoneità della disposizione ad integrare il parametro costituzionale.

Nel contesto tratteggiato si inserisce il ruolo svolto dal giudice comune allorché si trovi davanti ad un'antinomia tra una disposizione di legge ordinaria e la C.e.d.u. La prima operazione che dovrà essere compiuta sarà quella di tentare un'interpretazione conforme alla Convenzione. Qualora questa operazione non vada a buon fine, l'unica strada percorribile è quella dell'incidente di costituzionalità, per cui il giudice dovrà chiedere alla Corte costituzionale se la norma che intende applicare al caso concreto che sia contrastante con la C.e.d.u. violi l'art. 117, co. 1° Cost. Ciò che risulta, invece, assolutamente proibito al giudice è di disapplicare la norma interna e applicare direttamente la Convenzione. Un tale potere è, infatti confinato esclusivamente alle norme di diritto comunitario[8].

Nella delimitazione del parametro costituzionale, grande importanza riveste la Corte europea dei diritti nell'uomo. Infatti gli Stati membri del Consiglio d'Europa non si sono limitati alla individuazione di un elenco di diritti fondamentali, ma hanno anche previsto un sistema, di stampo giurisdizionale, per la loro tutela. Questo è, in prima battuta, reso operativo dai giudici nazionali dei singoli Stati, i quali sono chiamati ad applicare la Convenzione europea. In seconda battuta, è stata creata la Corte europea per i diritti dell'uomo, la quale ha tra le sue funzioni anche quella di garantire l'uniformità dell'applicazione e dell'interpretazione della C.e.d.u. Questa considerazione permette alla Corte costituzionale di rilevare

[8] In senso più ampio, il potere di disapplicazione della disposizione italiana in favore di una norma internazionale risulta riconosciuto esclusivamente per quanto riguarda il diritto dell'Unione europea. Anche in questo caso, il riconoscimento di un tale potere in capo ai giudici ordinari è arrivato dopo un lungo dibattito che ha visto per protagonisti la Corte costituzionale e la Corte di giustizia dell'allora comunità economica europea. L'atto finale della discussione è rappresentato da Corte cost., 8 giugno 1984, n. 170, cit. pronuncia con la quale l'art. 11 Cost. è stato riconosciuto come base giuridica valida per permettere un adeguamento automatico del nostro ordinamento rispetto alle fonti comunitarie di immediata applicazione.

come il parametro che vada ad integrare la norma interposta sia rappresentato non solo dalla disposizione della C.e.d.u. che viene invocata, ma anche dalla interpretazione data alla stessa dai giudici di Strasburgo[9].

Ovviamente, le decisioni della Corte costituzionale di cui si è ricostruita per sommi capi la struttura argomentativa non hanno mancato di suscitare un vivace dibattito in dottrina. In particolare, è stato oggetto di discussione il riferimento fatto dai giudici costituzionali alla giurisprudenza della Corte e.d.u. Infatti ad integrare il parametro di costituzionalità non è solo la disposizione della C.e.d.u. che si ritiene violata, ma anche l'interpretazione che della stessa ne dà la Corte. Questa seconda precisazione è tutt'altro che secondaria, alla luce della considerazione per cui la Corte e.d.u. tende molto spesso a fornire un'interpretazione estensiva o, alle volte, evolutiva dei diritti che intende tutelare. L'obiettivo perseguito dai giudici di Strasburgo è quello di garantire che i diritti umani non rimangano mai una mera enunciazione di principio, ma che vengano calati nel contesto reale in cui questi operano[10]. Il risultato di questa attitudine della Corte e.d.u. è stato quello, secondo alcuni, di mettere in crisi la distinzione tra legislazione e giurisdizione[11].

Proprio sui confini tra la funzione legislativa e quella giurisdizionale si è polarizzato il dibattito dottrinale in tema di validità delle sentenze della Corte e.d.u. a diventare parametro di legittimità costituzionale di una legge ordinaria. Infatti coloro che criticano la scelta fatta dai giudici costituzionali di lasciare che la norma interposta sia creata anche sulla base

[9] L'esistenza di un organo giurisdizionale che può essere adito direttamente dai singoli cittadini contro uno Stato per far rilevare la non corretta applicazione della Convenzione rappresenta il tratto distintivo più innovativo del sistema di tutela dei diritti approntato dal Consiglio d'Europa.

[10] Cfr. M. DANIELE, *Norme processuali convenzionali e margine di apprezzamento nazionale*, in *Cass. pen.*, 2015, p. 1692. V., anche Corte eur., 17 settembre 2009, Scoppola c. Italia, § 104.

[11] V. le considerazioni di P. FERRUA, *L'interpretazione della Convenzione europea dei diritti dell'uomo e il preteso monopolio della Corte di Strasburgo*, in *Proc. pen. giust.*, 2011, n. 4, p. 121.

della giurisprudenza della Corte e.d.u., lo fanno proprio sottolineando come, così facendo, si stia affidando ai giudici di Strasburgo un potere normativo che non hanno e che va a confliggere con la natura stessa della funzione giurisdizionale[12]. Prendendo le mosse da un discorso di carattere estremamente generale, questa dottrina rileva come l'interpretazione di una disposizione sia affidata al giudice, il quale, motivando, può scegliere, tra le interpretazioni possibili, quella che ritiene più corretta[13]. La scelta operata dal magistrato non è, però, mai vincolante per gli altri magistrati, anche quando la ricostruzione della norma sia compiuta da un organo di vertice come la Corte di cassazione a sezioni unite. Come stabilisce l'art. 101, co. 1° cost., i giudici sono soggetti soltanto alla legge. Trasportando queste considerazioni nel sistema della Corte europea dei diritti dell'uomo, si rileva come questa sia il giudice del caso concreto e non un giudice delle leggi. Per questo motivo, il valore precettivo delle sue pronunce è limitato alla controversia decisa; per tutte le altre, l'interpretazione data di una certa disposizione rimane esclusivamente un autorevole precedente da tenere in considerazione. Anche a voler invocare l'idea del precedente vincolante, prosegue questa dottrina, si rischia di cadere in un equivoco. Infatti il principio dello *stare decisis* impone ai giudici di conformarsi alla precedente decisione solo se il caso portato alla loro attenzione sia identico o analogo; qualora sia riconosciuta la sussistenza di elementi peculiari che valgano a differenziare la fattispecie, il vincolo viene meno[14]. L'affermazione compiuta dalla Corte costituzionale nelle sentenze gemelle sembra condurre a ritenere vincolante non il precedente, ma il significato della disposizione applicata alla fattispecie. Il risultato di una tale operazione è quello

[12] Cfr. P. FERRUA, *Il contraddittorio nella formazione della prova a dieci anni dalla sua costituzionalizzazione: il progressivo assestamento della regola e le insidie della giurisprudenza della Corte europea*, in *Arch. pen.*, 2008, n. 3, p. 28.

[13] V. ancora P. FERRUA, *L'interpretazione*, cit., pp. 119 s.

[14] Così si esprime P. FERRUA, *L'interpretazione*, cit., p. 119.

di rendere estremamente sfumati i confini tra il potere legislativo e quello giurisdizionale. L'interpretazione della Convenzione europea dei diritti dell'uomo effettuata dalla Corte di Strasburgo si trasformerebbe in legge e ai giudici comuni non resterebbe che interpretare la lettura delle disposizioni convenzionali compiuta dalla Corte.

Numerose critiche sono state indirizzate all'impostazione appena riferita. In primo luogo, è stata posta in discussione l'idea stessa che le sentenze della Corte e.d.u. non possano avere un'efficacia che si estenda oltre il singolo caso concreto. Infatti è stato fatto notare come le violazioni alla Convenzione possano derivare non soltanto da comportamenti illegittimi, ma anche da atti legittimi compiuti in ragione di una norma violatrice della Convenzione[15]. Ciò implicherebbe la possibilità che i giudici di Strasburgo si comportino in tali situazioni non come giudice del caso concreto ma come giudice delle leggi, la cui pronuncia non può non avere un valore generale. In secondo luogo, il richiamo all'art. 101, co. 2° Cost. risulterebbe in parte inconferente. Infatti si ammette pacificamente la possibilità per la legge di rinviare ad atti normativi "esterni" per completare la fattispecie da essa regolata. Questi atti normativi possono essere rappresentati da disposizioni di un ordinamento straniero, come nel caso dei rinvii operati nell'àmbito del diritto internazionale privato, oppure, appartenere al diritto comunitario, per il quale sussiste lo strumento del rinvio pregiudiziale *ex* art. 267 TFUE[16]. In questo contesto, non apparirebbe così irrazionale ammettere che l'interpretazione di una disposizione della Convenzione europea dei diritti dell'uomo effettuata dai giudici di Strasburgo possa andare a dare sostanza agli obblighi internazionali cui fa riferimento l'art.

[15] Cfr. S. CARNEVALE, *I rimedi contro il giudicato tra vizi procedurali e "vizi normativi"*, in *All'incrocio tra Costituzione e Cedu. Il ragno delle norme della Convenzione e l'efficacia interna delle sentenze di Strasburgo*, a cura di R. Bin – G. Brunelli – A. Pugiotto – P. Veronesi, Giappichelli, Torino, 2007, p. 61; G. UBERTIS, *La "rivoluzione d'ottobre" della Corte costituzionale e alcune discutibili reazioni*, in *Cass. pen.*, 2012, p. 21.

[16] Ancora, G. UBERTIS, *op. cit.*, p. 22.

117, co. 1° Cost. In terzo luogo, l'eventuale rischio di una difficoltà di adattamento degli orientamenti della Corte e.d.u. nel nostro ordinamento potrebbe essere risolta alla luce della dottrina del "margine di apprezzamento". Infatti in una pronuncia di poco successiva alle sentenze gemelle, è stato precisato come se è vero che la Corte costituzionale non può sostituirsi alla Corte di Strasburgo per quanto riguarda l'interpretazione della C.e.d.u., è anche vero che i giudici costituzionali hanno il dovere di valutare «in quale misura il prodotto dell'interpretazione della Corte europea si inserisca nell'ordinamento costituzionale italiano[17]».

Recentemente, la Corte costituzionale ha avuto modo di chiarire ulteriormente la sua posizione sul tema, effettuando alcune utili precisazioni circa il valore delle sentenze della Corte di Strasburgo all'interno dell'ordinamento italiano[18]. In tale pronuncia, i giudici costituzionali, infatti, chiariscono come, nell'opera di interpretazione delle disposizioni della Convenzione, i giudici comuni debbano fare riferimento esclusivamente alla giurisprudenza consolidata della Corte e.d.u. Solo questa può essere utilizzata sia come strumento per definire l'esatto perimetro del diritto tutelato dalla C.e.d.u. sia per integrare il parametro costituzionale allorché si sospetti un'antinomia tra una norma interna e la Convenzione[19].

[17] Così, Corte cost., 4 dicembre 2009, n. 317 in *Giur. cost.*, 2009, pp. 4747 ss.

[18] Ci si riferisce a Corte cost., 26 marzo 2015, n. 49 in *Giur. Cost.*, 2015, pp. 391 ss. Per un commento a tale pronuncia, tra i tanti, si segnalano quelli di M. BIGNAMI, *Le gemelle crescono in salute: la confisca urbanistica tra Costituzione, C.e.d.u., e diritto vivente*, in *Dir. pen. cont.*, 2015, n. 2., pp. 288 ss.; D. PULITANÒ, *Due approcci opposti sui rapporti tra Costituzione e Cedu in materia penale. Questioni lasciate aperte da Corte cost. n. 49/2015*, in *Dir. pen. cont.*, 2015, n. 2, pp. 318 ss.; F. VIGANÒ, *Osservazioni a primissima lettura su Corte cost., sent. 26 marzo 2015, n. 49, Pres. Criuscolo, Red. Lattanzi, in materia di confisca di terreni abusivamente lottizzati e proscioglimento per prescrizione*, in *Dir. pen. cont.*, 2015, n. 2, pp. 333 ss.; V. ZAGREBELSKY, *Corte cost. n. 49 del 2015, giurisprudenza della Corte europea dei diritti umani, art. 117 Cost., obblighi derivanti dalla ratifica della Convenzione*, in www.osservatorioaic.it, pp. 1 ss.

[19] Rileva, inoltre, F. VIGANÒ, *Osservazioni*, cit., p. 337 come la Corte costituzionale sembrerebbe aver ammesso un obbligo di conformazione alle pronunce dei giudici di Strasburgo a carico dei giudici nazionali, tutte le volte in cui sussista una giurisprudenza europea consolidata in merito ad una certa questione.

Un tentativo di ricomporre il dibattito appena ricostruito può, forse, derivare proprio dalla valorizzazione del "margine di apprezzamento", inteso come strumento che possa riequilibrare i rapporti tra l'ordinamento italiano e il sistema della C.e.d.u.[20]. Con l'espressione margine di apprezzamento, si fa riferimento alla possibilità per i singoli Stati del Consiglio d'Europa di poter apprestare, entro, appunto, un determinato margine, una diversa tutela dei diritti enunciati nella C.e.d.u. La nascita di tale dottrina è dovuta all'idea per cui la Corte di Strasburgo cerca sempre di unire due esigenze tra di loro confliggenti: fornire un'interpretazione uniforme della C.e.d.u., nonostante le rilevanti differenze che sussistono tra i vari ordinamenti. Nel fare ciò, la Corte e.d.u. allarga o diminuisce lo spazio di manovra affidato ai singoli Stati. Nel primo caso, fa riferimento alla c.d. *better position* in cui uno Stato si trova rispetto ai giudici di Strasburgo nella scelta delle modalità più opportune per garantire piena tutela ad un determinato diritto fondamentale[21]. Viceversa, allorché intenda restringere il margine di apprezzamento si richiama, di norma, al c.d. *consensus standard*, ossia alla sussistenza di un modello di garanzia tra la maggioranza degli Stati membri del Consiglio d'Europa in relazione alle modalità di tutela di un determinato diritto[22]. Tuttavia, al netto della generica definizione data dalla stessa Corte e.d.u., alcuni hanno cercato di raffinare il criterio in base al quale sia possibile per un giudice comune di invocare il margine di apprezzamento.

Una prima premessa che deve essere svolta riguarda la sussistenza di una pronuncia della Corte europea dei diritti dell'uomo in un caso uguale a quello oggetto della decisione. In questo caso, il giudice non avrebbe molto spazio di manovra, dovendo necessariamente

[20] Cfr. M. DANIELE, *op. cit.*, p. 1696.

[21] V., ad esempio, Corte eur., 16 dicembre 2010, A, B e C c. Irlanda, § 223 in tema di normativa riguardante l'aborto; Corte eur., 7 dicembre 1976, Handyside c. Regno Unito, §§ 48 ss.

[22] V., Corte eur., 26 aprile 1979, Sunday Times c. Regno Unito, §§ 48 ss.

uniformarsi alla decisione presa dai giudici di Strasburgo. Una decisione contraria condurrebbe molto facilmente ad un nuovo intervento della Corte e.d.u., la quale, con molta probabilità, ribadirebbe il suo indirizzo giurisprudenziale. Diversamente, il margine di apprezzamento può risultare utile nel caso in cui la fattispecie portata davanti al giudice sia simile a quanto già deciso in sede sovranazionale. Per questa eventualità, la dottrina in discorso, contempla due scenari.

Una prima eventualità è quella in cui vi sia una norma convenzionale derivante da una pronuncia della Corte di Strasburgo in un caso che, avendo particolari elementi di differenziazione, non sia del tutto identico a quello su cui il giudice nazionale sia chiamato a decidere. In questo caso, l'autorità giurisdizionale potrebbe, proprio con la tecnica del *distinguishing*, valorizzare le differenze tra le due fattispecie per applicare esclusivamente la norma nazionale al posto di quella convenzionale[23].

Una seconda eventualità si ha, invece, nel caso in cui vi sia una norma convenzionale riguardante casi analoghi a quello portato all'attenzione del magistrato decidente. In tal caso, l'unica possibilità per lo stesso di emanciparsi dalla giurisprudenza della Corte europea dei diritti dell'uomo sembrerebbe essere quella di evocare i c.d. contro-limiti. Tuttavia, una tale possibilità sembrerebbe più teorica che pratica: pare difficile immaginare una norma convenzionale che sia in radicale contrasto con i princìpi costituzionali[24]. In questi casi, il margine di apprezzamento potrebbe svolgere un'importante funzione di riequilibratura tra ordinamento nazionale e convenzionale. Infatti qualora sussistesse una norma nazionale che, pur non essendo identica a quella convenzionale, fosse in grado di fornire al diritto protetto

[23] Cfr. M. DANIELE, *op. cit.*, p. 1696.

[24] In tal senso, v. E. LAMARQUE, *Le relazioni tra l'ordinamento nazionale, sovranazionale e internazionale nella tutela dei diritti*, in *Dir. pubbl.*, 2013, pp. 716 ss.

un grado di tutela equivalente, il giudice nazionale potrebbe decidere di dare prevalenza alla normativa nazionale a scapito di quella scaturente dal sistema convenzionale[25].

Di natura nettamente differente è il discorso riguardante il valore da assegnare alla Carta di Nizza nel nostro ordinamento. In primo luogo, bisogna rilevare come il Trattato di Lisbona all'art. 6, co. 1° assegni espressamente alla Carta dei diritti fondamentali dell'Unione europea «lo stesso valore giuridico dei trattati». Teoricamente, una tale disposizione dovrebbe comportare la diretta applicazione della Carta di Nizza nel nostro ordinamento e la sua primazia rispetto al diritto italiano nelle materie di competenza dell'Unione europea. Ulteriore conseguenza sarebbe anche quella della possibilità per il giudice di poter disapplicare la norma italiana che sia contrastante con una previsione della Carta di Nizza[26]. Questa ricostruzione è stata incidentalmente riconosciuta valida dalla Corte costituzionale nella sentenza 11 marzo 2011, n. 80, nella quale i giudici costituzionali, dopo aver definito i rapporti tra il nostro ordinamento, la C.e.d.u. e la Carta di Nizza ammettono che quest'ultima sia parte integrante del diritto dell'Unione europea. Ciò comporta non solo il riconoscimento per la Carta dei diritti dell'Unione europea della medesima posizione nella gerarchia delle fonti dei trattati europei ma anche il suo limitato effetto diretto. Infatti, come stabilito dall'art. 51 della stessa Carta, «le disposizioni della presente Carta si applicano alle istituzioni e agli organi

[25] In tal senso, M. DANIELE, *op. cit.*, p. 1698.

[26] La questione, tuttavia, si complica ulteriormente a causa dei complessi rapporti tra la Carta dei diritti fondamentali dell'Unione europea e la C.e.d.u.: infatti, l'art. 52 Carta di Nizza contiene una clausola di equivalenza in merito ai diritti tutelati da quest'ultima e dalla C.e.d.u. Tale disposizione prevede che tutte le volte in cui ci siano diritti equivalenti nelle due Carte dei diritti, il significato e la portata degli stessi siano uguali a quelli conferiti dalla C.e.d.u. Le spiegazioni della Carta di Nizza precisano, inoltre, che la delimitazione dei diritti protetti dalla Convenzione europea dei diritti dell'uomo sarà compiuta non soltanto sulla base del testo della stessa ma anche sulla base della giurisprudenza della Corte europea dei diritti dell'uomo. Considerando che tutti i diritti contenuti nella C.e.d.u. sono presenti nella Carta di Nizza in forme spesso molti simili, alcuni commentatori hanno ritenuto che la Convenzione fosse stata sostanzialmente inglobata nel diritto dell'Unione europea. Conseguenza di tale affermazione sarebbe quella di permettere al giudice ordinario di disapplicare la norma interna contrastante con la C.e.d.u. Questa lettura è stata respinta dalla Corte costituzionale nella sentenza 11 marzo 2011, n. 80, in *Giur. cost.*, 2011, pp. 1224 ss. nella quale i giudici costituzionali hanno rilevato come la C.e.d.u. abbia una vocazione generale, mentre, invece la Carta di Nizza sia applicabile solo nelle materie di competenza dell'Unione europea.

dell'Unione nel rispetto del principio di sussidiarietà come pure agli Stati membri esclusivamente nell'attuazione del diritto dell'Unione[27]».

[27] Per ulteriori considerazioni, v. P. GIANNITI, *La «comunitarizzazione» della «carta» a seguito del trattato di Lisbona*, in *I diritti fondamentali nell'Unione europea. La Carta di Nizza dopo il Trattato di Lisbona*, a cura di P. Gianniti, Zanichelli, Bologna, 2015, pp. 366 ss.

2. Il diritto alla riservatezza in àmbito nazionale ed europeo

Riprendendo le fila del discorso interrotto per dar conto del valore che la C.e.d.u. e il diritto dell'Unione europea hanno nel nostro ordinamento, si può affermare come, tra i valori messi in pericolo dalle operazioni di *digital forensics*, quello della riservatezza sia sicuramente uno dei primi a venire in gioco, tenendo anche conto che gli ulteriori diritti rilevanti, ossia l'inviolabilità del domicilio e delle comunicazioni, ne potrebbero costituire una specificazione.

Volendo affrontare il discorso facendo riferimento alla normativa italiana, deve essere rilevato come all'interno della Costituzione non si rinvenga alcuna disposizione che faccia espresso riferimento alla tutela della riservatezza o della *privacy*[28]. Questa mancanza ha comportato numerosi problemi, tra cui, quello, appunto dell'individuazione di un appiglio costituzionale che possa giustificare la protezione di un tale diritto.

Da un punto di vista di carattere estremamente generale tanto la dottrina quanto la giurisprudenza costituzionale riconoscono l'art. 2 Cost. come il riferimento di natura costituzionale più opportuno in tema di tutela della riservatezza[29]. Tuttavia, scendendo più nello specifico vi sono da segnalare almeno due diverse correnti di pensiero sul punto. Secondo una prima, l'art. 2 Cost., laddove faccia riferimento ai «diritti inviolabili dell'uomo» che la Repubblica è chiamata a riconoscere e a garantire, conterrebbe una clausola di carattere generale idonea a permettere un costante aggiornamento del catalogo dei beni giuridici protetti

[28] Viceversa, come fatto notare da A. GAITO – S. FÙRFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, in *I princìpi europei del processo penale*, a cura di A. Gaito, Dike giuridica editrice, Roma, 2016, p. 369 le fonti sovranazionali riconoscono direttamente il diritto alla riservatezza. Questo è, infatti, sancito tanto dall'art. 12 della Dichiarazione universale dei diritti umani, quanto dall' art. 17 Patto internazionale sui diritti civili e politici. Per quanto riguarda, invece, la Convenzione europea dei diritti dell'uomo e la Carta di Nizza v. *infra* nel testo.

[29] Cfr. S. FÙRFARO, *Il diritto alla riservatezza*, in *Riservatezza ed intercettazioni tra norma e prassi*, a cura di A. Gaito, 2011, Aracne, Roma, p. 38.

dalla Costituzione e, quindi, il riconoscimento di nuovi diritti da tutelare[30]. Tra queste nuove posizioni giuridiche soggettive, vi sarebbe anche quel fascio di diritti e facoltà che possono essere ricondotti al concetto di riservatezza. Per cui, secondo questo orientamento, l'art. 2 Cost. costituirebbe il solo fondamento normativo della tutela della *privacy*.

Diversamente, altri studiosi, insieme alla giurisprudenza della Corte costituzionale, riconoscono come la disposizione in commento non sia sufficiente da sola ad offrire una piena ed effettiva protezione della riservatezza, a causa della sua eccessiva genericità[31]. Per questo motivo, si ammette la necessità di integrare l'art. 2 Cost. con le disposizioni costituzionali che più si avvicinano alla situazione concreta da tutelare. In altri termini, si ammette la possibilità di offrire un'interpretazione relativamente ampia di alcune libertà fondamentali, le quali vengono viste attraverso il prisma dell'art. 2 Cost.[32].

Tra le prime pronunce ad utilizzare tale approccio, merita di essere segnalata l'ormai risalente sentenza 6 aprile 1973, n. 34 della Corte costituzionale, avente per oggetto la disciplina delle intercettazioni di comunicazioni del codice di procedura penale abrogato[33]. Come riconosciuto da alcuni commentatori, in tale pronuncia la Corte si occupa del profilo della *privacy* riguardante la riservatezza delle comunicazioni[34]. Questo viene riconosciuto come «connaturale ai diritti della personalità definiti inviolabili dall'art. 2 Cost.». Tuttavia, proprio l'indeterminatezza del livello di tutela assicurato dal citato articolo alla riservatezza rende

---

[30] Cfr. *ex multis*, A. BARBERA, sub *art. 2*, in *Commentario alla costituzione*. *Princìpi fondamentali*, a cura di G. Branca, Zanichelli, Bologna, 1975, pp. 80 ss.; In relazione al diritto alla riservatezza, v. F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. dir. proc. pen.*, 1967, pp. 1094 s.

[31] In tal senso, A. CATAUDELLA, *Riservatezza (diritto alla) I) diritto Civile*, in *Enc. giur. Treccani*, Roma, 1994, pp. 2 s.; P. GROSSI, *Inviolabilità dei diritti*, in *Enc. dir.*, Giuffrè, Milano, 1972, vol. XXIII, pp. 728 s.

[32] C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, Torino, 2007, pp. 83 ss.

[33] V. Corte cost., 6 aprile 1973, n. 34 in *Giur. cost.*, 1973, pp. 316 ss. con nota di V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*.

[34] In tal senso, F.B. MORELLI, *La giurisprudenza costituzionale italiana tra diritto alla riservatezza e potere di controllo sulle informazioni personali*, in *Protezione dei dati personali e accertamento penale*, a cura di D. Negri, Aracne, Roma, 2007, p. 34.

necessario il richiamo anche all'art. 15 Cost., nel quale vi è, invece, un bilanciamento tra le esigenze di libertà e quelle di repressione dei reati[35]. Questo schema di ragionamento verrà successivamente replicato anche per tutte quelle fattispecie per le quali risulta difficile trovare un immediato referente costituzionale.

La sentenza 12 aprile 1973, n. 38 sempre della Corte costituzionale, ne offre un'esemplificazione migliore[36]. In tal caso, l'equilibrio era da ritrovare tra le esigenze di tutela dell'immagine del singolo e quelle della libertà di stampa. Mentre l'ultima trova espressa tutela nell'art. 21 Cost., la prima è priva di garanzie esplicite. Per questo motivo, i giudici costituzionali ancorano il diritto alla riservatezza dell'immagine al combinato disposto dagli artt. 2, 3, co. 2° e 13, co. 1° Cost., i quali «riconoscono e garantiscono i diritti inviolabili dell'uomo, fra i quali rientra quello [...] della propria [...] riservatezza».

Senza voler ripercorrere tutta la giurisprudenza costituzionale in materia, risulta utile rilevare come la Corte costituzionale, in una sentenza nettamente successiva rispetto agli arresti citati, utilizzi ancora lo schema di ragionamento sommariamente descritto. Il riferimento è alla già citata sentenza Corte cost. 24 aprile 2002, n. 135[37]. Allorché si è posta la questione di definire compiutamente le situazioni soggettive che vengono in rilievo per quanto attiene alla predisposizione di videoriprese all'interno del domicilio, la Corte sottolinea come l'inviolabilità del domicilio, insieme alla libertà e alla segretezza delle comunicazioni costituiscano due profili di un più ampio diritto che è quello alla riservatezza. Questo diritto, a causa delle sue numerose sfaccettature, non può essere ricondotto ad una singola disposizione, ma attraversa numerose norme costituzionali[38]. Tra le due opzioni esegetiche riferite,

[35] V., ancora, F.B. MORELLI, *op. cit.*, p. 35.

[36] V. Corte cost., 12 aprile 1973, n. 38, in *Giur. cost.*, 1973, pp. 354 ss.

[37] Pubblicata in *Giur. cost.*, 2002, cit. Sul punto, si rimanda alle considerazioni svolte nel Cap. II, § 2.

[38] Cfr. F.B. MORELLI, *op. cit.*, p. 40.

la seconda, grazie anche alla maggiore tutela che riesce offrire al diritto alla riservatezza, sembrerebbe essere quella da accettare.

Volgendo lo sguardo alla tematica della delimitazione del concetto di riservatezza, si può concordare con quegli studiosi che riconoscono come il cuore del diritto alla riservatezza sia rappresentato dal diritto ad essere lasciati soli, ossia dall'idea per cui ciascuno di noi ha diritto alla tutela di una sfera intima che non può essere violata da parte dell'autorità pubblica[39].

A partire da questo nucleo fondamentale, si dipanano diverse strade che vanno a riconoscere rilevanza a diverse posizioni giuridiche soggettive, come il diritto all'identità personale, all'immagine, al decoro, alla reputazione, alla tranquillità individuale e alla protezione dei dati personali[40]. Tra queste, quella che maggiormente interessa nel presente lavoro è l'ultima prospettiva citata: quella riguardante la protezione dei dati di carattere personale. Infatti il processo penale, avendo come obiettivo quello di tentare una, seppur imperfetta, ricostruzione di un accadimento passato, funge da recettore di un gran numero di dati di carattere personale[41]. Inoltre, gli atti di acquisizione di evidenze di carattere informatico si concretizzano nella loro totalità come operazioni di estrazione o di intercettazione di dati informatici riguardanti un determinato soggetto[42].

A livello di legislazione ordinaria, è il d.lgs. 30 giugno 2003, n. 196 rubricato codice in materia di protezione dei dati personali ad occuparsi di tale aspetto. Questi definisce, all'art.

---

[39] Cfr. A. CATAUDELLA, *op. cit.*, p. 1; C. MARINELLI, *op. cit.*, pp. 82 s. Per una prospettiva di carattere storico sul tema, si rimanda a A. BALDASSARRE, Privacy *e costituzione: l'esperienza statunitense*, Bulzoni, Roma, 1967, pp. 9 ss.

[40] V. in tal senso, S. CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in *Protezione dei dati personali*, cit., p. 10. Per un'illustrazione delle problematiche connesse all'evoluzione del concetto di riservatezza causato dallo sviluppo tecnologico, v. A. CISTERNA, *Cedu e diritto alla privacy*, in *I princìpi europei*, cit., pp. 193 ss.

[41] Così, S. CARNEVALE, *op. cit.*, p. 5.

[42] Cfr. Cap. II, §§ 3, 4.

2, co. 1° lett. *b*) Codice *privacy*, come dato personale «qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale». Viceversa, costituisce trattamento, sempre a norma dell'art. 2, co. 1°, lett. *a*) Codice *privacy*, «qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati». Allorché debba essere effettuata una delle operazioni citate, è necessario che il titolare dei dati personali oppure il soggetto pubblico o privato incaricato di decidere sulle modalità e finalità del trattamento, agiscano seguendo le procedure previste dal Codice *privacy*. Sul rispetto della normativa citata, vigila il Garante per la protezione dei dati personali[43].

Ampliando l'orizzonte della presente trattazione all'àmbito europeo, viene in gioco, in prima battuta, la tutela della riservatezza apprestata dalle fonti dell'Unione europea. Questa viene garantita su due livelli: da un lato, attraverso la Carta dei diritti fondamentali dell'Unione europea e, dall'altro lato, per il tramite del diritto dell'Unione derivato, ossia regolamenti, direttive e decisioni.

La Carta di Nizza prende in considerazione il diritto alla vita privata e alla riservatezza agli artt. 7, 8. La prima di queste disposizioni ricalca sostanzialmente l'art. 8, § 1 C.e.d.u.: la

[43] Il tema dell'utilizzo dei dati cui fa riferimento il Codice *privacy* sarà ripreso nel Cap. IV, § 3.

differenza più rilevante è data dall'utilizzo del termine comunicazioni invece di corrispondenza[44]. Il leggero cambio di formulazione ha inteso recepire gli esiti cui è giunta la giurisprudenza della Corte europea dei diritti dell'uomo che, come si vedrà, ha assegnato al termine corrispondenza un significato molto ampio, idoneo a ricomprendere tutte le tipologie di comunicazioni.

Per quanto riguarda l'interpretazione dell'art. 7 Carta di Nizza, non può non richiamarsi, almeno in prima battuta, alle considerazioni che verranno effettuate in tema di tutela della vita privata a norma della C.e.d.u. Infatti l'art. 52, co. 3° Carta di Nizza prevede una clausola di equivalenza tra le garanzie apprestate dalla stessa e quelle contenute nella C.e.d.u. in tutti quei casi in cui determinati diritti siano oggetto di tutela da parte di entrambe le Carte.

Diverso è il discorso per quanto riguarda l'art. 8 Carta di Nizza, il quale, assumendo come punto di partenza il diritto alla vita privata, estende la sua tutela ad altre e diverse fattispecie concrete: ci si riferisce, in particolare, alla tematica dei dati personali. Come è stato fatto notare dalla dottrina, sicuramente l'art. 8, § 1 C.e.d.u. costituisce la base di partenza per la definizione della tutela dei dati personali; tuttavia, è l'art. 8 Carta di Nizza che sancisce la nascita di un vero e proprio nuovo diritto, separato dal quello alla riservatezza, quale è quello, appunto, della c.d. *data protection*[45].

La *ratio* sottesa ad un tale tipo di tutela è da ricercarsi nei mutamenti sociali e, soprattutto, nell'emersione della società digitalizzata. Infatti ciascuno di noi nella sua vita quotidiana dissemina tracce del proprio passaggio in rete e non solo. La collezione e l'analisi di

[44] Come sottolineato da M. Murgo, *Diritti di libertà*, in *I diritti fondamentali nell'Unione europea. La Carta di Nizza dopo il Trattato di Lisbona*, a cura di P. Gianniti, Zanichelli, Bologna, 2015, p. 763, la differenza di terminologia usata riflette semplicemente il diverso momento storico in cui le due Carte dei diritti sono state compilate.

[45] Anche in questo caso, la necessità di codificare un tale diritto sorge in stretta connessione con i mutamenti della società contemporanea: l'avvento delle nuove tecnologie ha reso necessario porre sotto controllo il flusso di dati che ciascuno di noi dissemina giornalmente. Cfr. M. Murgo, *op. cit.*, p. 776.

tutti questi dati può fornire una rilevante serie di informazioni sulle abitudini di vita, sulle opinioni politiche o religiose e sullo stato di salute di un individuo. Proprio per tale ragione si è reso necessario assicurare una qualche forma di controllo sulla circolazione di queste informazioni. In relazione a questo obiettivo, la semplice tutela ordinariamente apprestata al diritto alla riservatezza è apparsa poco efficace. Infatti per quanto si possa espandere il concetto di domicilio o di vita privata, tale forma di tutela rischia di lasciare prive di effettiva protezione tutta una molteplicità di situazioni di fatto.

Dal canto suo, la Comunità europea prima e l'Unione europea poi si sono occupati a più riprese del tema. La prima direttiva è stata la 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. A questa sono seguite la direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, e la direttiva 2002/58/CE che si occupa del trattamento dei dati personali e della tutela della vita privata nel settore delle comunicazioni elettroniche. Ultimamente si segnalano: il regolamento 2016/679/UE, che sostituisce la citata direttiva 95/46/CE, nonché la direttiva 2016/680/UE riguardante il trattamento dei dati personali da parte delle autorità competenti per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali; e la direttiva 2016/681/UE, avente per oggetto l'acquisizione dei dati relativi al codice di prenotazione sempre per finalità di carattere penale[46].

Ad un primissimo sguardo, i testi normativi citati sembrerebbero avere rilevanza esclusivamente in relazione ad alcuni profili del presente lavoro. Infatti sia il regolamento 2016/679/UE sia la direttiva 2016/680/UE definiscono dato personale «qualsiasi informazione

[46] Per una generale ricognizione dei testi normativi citati, v. F. PIZZETTI, Privacy *e diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016, pp. 147 ss.

riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online [...]». Il richiamo ai dati di ubicazione e all'identificativo *online* di un soggetto pare fare riferimento a dati di carattere informatico che possono essere raccolti dall'autorità giudiziaria. Dalla lettura dei considerando, emerge come tra i princìpi cui dovrebbe ispirarsi il trattamento di tali informazioni dovrebbe esserci anche quello di neutralità tecnologica, per cui l'applicazione della normativa europea è indipendente dalle modalità tecnologiche usate per la protezione dei dati[47]. Inoltre, sempre nei considerando, si chiarisce da un lato come la raccolta dei dati precedentemente definiti sia permessa solo per finalità di prevenzione, indagine, accertamento e perseguimento dei reati e, dall'altro, che l'intervento di uno Stato membro sul tema dovrà avvenire tramite un atto normativo che sia chiaro, preciso e di prevedibile applicazione ai soggetti interessati[48]. Considerando la recentissima emanazione dei due atti normativi citati e la mancanza di una normativa di recepimento per la direttiva 2016/680/UE, risulta al momento difficile giudicare quali effetti avranno questi provvedimenti sulla raccolta delle prove di carattere informatico.

Sempre in relazione all'azione europea tesa a garantire una piena tutela dei dati personali, merita un accenno anche la direttiva 2006/24/CE, la quale ha modificato la direttiva 2002/58/CE che imponeva agli Stati membri di adottare una particolare disciplina in tema di conservazione di dati comunicativi esterni per finalità di repressione dei reati. Tra le motivazioni che hanno mosso l'azione europea, una è da ritrovarsi nella lotta al fenomeno del

[47] In relazione al principio di neutralità tecnica nell'ordinamento italiano, v. G. LASAGNI, *L'uso di captatori informatici (*trojans*) nelle intercettazioni "fra presenti"*, in *www.penalecontemporaneo.it*, pp. 11 ss.

[48] Cfr. considerando nn. 29, 34 direttiva 2016/680/UE.

terrorismo internazionale, il quale, dopo gli attentati compiuti a Madrid e a Londra, si è mostrato in netta crescita[49].

L'art. 1 della direttiva citata rendeva immediatamente chiaro quale fosse lo scopo della normativa: uniformare le legislazioni nazionali riguardanti la conservazione dei dati generati automaticamente dai sistemi comunicativi al fine di permettere una loro utilizzazione per finalità di repressione dei reati. Come specificato in dottrina, la premessa principale di una tale regolamentazione era da ritrovarsi nella constatazione circa l'importanza nelle investigazioni di carattere penale dei dati raccolti e immagazzinati da parte degli operatori telefonici o dai fornitori di connettività per finalità loro proprie[50]. La prima indicazione contenuta nella direttiva è stata quella di imporre un obbligo di conservazione di tali dati per un periodo che varia da un minimo di sei mesi fino a due anni per i dati telefonici e per un periodo di sei mesi per quanto riguarda le informazioni registrate dagli *Internet Service Provider* (ISP). L'art. 5 della direttiva si occupava di dare una definizione più precisa dei dati che devono essere conservati. Questi erano raggruppati in sei diverse categorie le quali facevano riferimento ai dati necessari per poter identificare la fonte della comunicazione, il destinatario, la data e l'ora della stessa, la sua tipologia, le attrezzature utilizzate e, infine, il luogo in cui si trova l'apparecchiatura mobile utilizzata. Inoltre, data la delicatezza delle informazioni conservate dagli operatori telefonici e dagli ISP, si imponeva la predisposizione delle opportune misure di sicurezza per evitarne la cancellazione e l'alterazione tanto incidentale quanto illecita. Per quanto atteneva all'accesso ai dati da parte dell'autorità, da un lato, si

[49] V. G. Di Paolo, *Le novità del Parlamento Europeo e Consiglio – direttiva del 15 marzo 2006, 2006/24/CE, riguardante la conservazione dei dati generati e trattati nell'ambito della fornitura dei servizi accessibili al pubblico di comunicazione elettronica e di reti pubbliche di comunicazione che modifica la direttiva 2002/58/CE,* in *Cass. pen.*, 2006, pp. 3582 s.

[50] Cfr. G. Di Paolo, *op. cit.*, p. 2197.

imponeva la creazione di un *database* idoneo a permettere la trasmissione immediata dei dati rilevanti per un'indagine penale e, dall'altro lato, la predisposizione di procedure di controllo che fossero ispirate ai princìpi di necessità e di proporzionalità. Infine, sempre al fine di salvaguardare tali dati si imponeva a ciascuno Stato membro l'obbligo di nominare un'autorità competente a vigilare circa il corretto uso di tali informazioni.

La direttiva brevemente tratteggiata è stata oggetto di una rilevante pronuncia da parte della Corte di Giustizia dell'Unione europea, la quale ne ha sancito la contrarietà, tra le altre cose, alla Carta di Nizza[51].

Più nello specifico, la sentenza 8 aprile 2014 della Corte di Giustizia dell'Unione europea è stata pronunciata a seguito di due ricorsi pregiudiziali presentati uno dalla *High Court* della Repubblica d'Irlanda e l'altro dal *Verfassungsgerichtshof* della Repubblica d'Austria. Tra le varie questioni sollevate, quelle che maggiormente sono rilevanti ai fini del discorso che si sta conducendo sono due: la prima, riguardante la compatibilità della direttiva 2006/24/CE con il diritto alla vita privata così come tutelato dagli artt. 7 Carta di Nizza e 8 C.e.d.u.; la seconda, la legittimità della citata direttiva in relazione alla tutela dei dati personali così come protetti dall'art. 8 Carta di Nizza.

Nelle motivazioni della sentenza, la Corte di Giustizia, dopo aver sommariamente riassunto il contenuto della direttiva ne va a controllare la legittimità alla luce del diritto alla riservatezza e a quello del trattamento dei dati personali. In primo luogo, i giudici del Lussemburgo si interrogano circa la possibilità o meno che la direttiva 2006/24/CE possa integrare una violazione del diritto sancito dall'art. 7 Carta di Nizza. Per quanto attiene al diritto

[51] Ci si riferisce alla nota sentenza della Corte di giustizia dell'Unione europea ECLI:EU:C:2014:238. La sentenza citata e le conclusioni dell'avvocato generale Pedro Cruz Villalón sono consultabili sulla banca dati ufficiale della Corte di giustizia all'indirizzo http://curia.europa.eu/

alla vita privata la risposta è affermativa sulla base di numerose argomentazioni. Innanzitutto, la mera conservazione dei dati indicati all'art. 5 § 1 della citata direttiva costituisce un'ingerenza nel diritto al rispetto della vita privata. Ciò in quanto quei dati sono afferenti alla vita privata degli individui. Non rileva, secondo la Corte né l'effettiva sussistenza di una lesione concreta al diritto alla vita privata né la sensibilità o meno dei dati raccolti. È la registrazione di tali informazioni da parte degli operatori telefonici o dei fornitori di connettività a costituire, di per sé, un'ingerenza nel diritto tutelato dall'art. 7 Carta di Nizza. Da questo punto di vista, il potere concesso alle autorità pubbliche di poter ottenere i dati delle comunicazioni registrati in occasione delle stesse andrebbe a formare un'ulteriore ingerenza nella vita privata dei cittadini dell'Unione europea.

In secondo luogo, i giudici del Lussemburgo si occupano del rapporto tra la direttiva in commento e l'art. 8 Carta di Nizza, che tutela il corretto trattamento dei dati personali. Sul tema, la Corte rileva anche in questo caso un'ingerenza da parte della direttiva in relazione all'art. 8 Carta di Nizza. Infatti la mera raccolta di una tale quantità di dati personali costituisce una violazione della protezione degli stessi apprestata dalla Carta di Nizza. Inoltre, come rilevano sia la Corte sia l'avvocato generale nelle sue conclusioni, il fatto che la raccolta di tali dati avvenga senza che gli interessati ne siano a conoscenza genera una diffusa «sensazione che la loro vita privata sia oggetto di costante sorveglianza[52]».

Tuttavia, l'indagine sull'esistenza o meno di un'ingerenza nei diritti sanciti dalla Carta di Nizza non comporta l'automatica illegittimità della direttiva. Infatti, dopo aver precisato che sussiste una compressione dei diritti di cui agli artt. 7, 8 Carta di Nizza, la Corte si preoccupa di controllare la legittimità dell'atto normativo alla luce della clausola di salvezza di cui

[52] Cfr. ECLI:EU:C:2014:238, § 37.

all'art. 52, § 1 Carta di Nizza. Questa disposizione ammette limitazioni ai diritti fondamentali dell'Unione europea, qualora queste siano previste da una legge, rispettino il contenuto essenziale del diritto e, in adesione al principio di proporzionalità, siano necessarie per garantire il perseguimento di interessi generali o la tutela di diritti o libertà altrui.

Per quanto riguarda l'osservanza del contenuto essenziale dei diritti di cui agli artt. 7, 8 Carta di Nizza, la Corte riconosce come la direttiva 2006/24/CE sia rispettosa di tale requisito. Infatti, da un lato, i dati raccolti non permettono di ottenere il contenuto delle comunicazioni dei cittadini dell'Unione europea e, dall'altro lato, viene imposto ai fornitori di servizi di telecomunicazione di garantire degli standard minimi di protezione dei dati raccolti e registrati.

Sulla giustificazione della direttiva in commento in relazione al perseguimento da parte della stessa di finalità di carattere generale, la Corte si preoccupa di andare alla ricerca dell'effettivo obiettivo perseguito dalle disposizioni. Infatti, pur riconoscendo come la direttiva sia finalizzata a garantire l'uniformità nella conservazione dei dati del traffico telefonico o elettronico, parimenti, evidenzia come il vero obiettivo della disposizione sia quella di fornire all'autorità pubblica un utile strumento per la repressione dei reati. Ciò in quanto la creazione di standard di conservazione è imposta per rendere più semplice la comunicazione dei dati raccolti dagli operatori di telecomunicazione alle autorità pubbliche. In quest'ottica, la Corte riconosce come le finalità di tutela della pubblica sicurezza possano astrattamente legittimare misure come quelle previste dalla direttiva 24/2006/CE. Ciò soprattutto alla luce della riemersione del fenomeno terroristico in Europa.

Riconosciuta la mancata lesione del contenuto essenziale dei diritti di cui agli artt. 7, 8 Carta di Nizza e la legittimità dei fini posti alla base della compressione dei diritti in di-

scorso, la Corte passa ad occuparsi del rispetto del principio di proporzionalità. Questo impone di controllare che gli atti dell'Unione europea siano idonei a perseguire le finalità legittime per cui sono stati emanati. Tuttavia, allorché vengano in gioco dei diritti fondamentali, la discrezionalità del legislatore europeo è limitata. Infatti, nell'emanazione di atti che possono ledere tali diritti, deve essere presa in considerazione «il settore interessato, la natura del diritto garantito dalla Carta, la natura e la gravità dell'ingerenza nonché la finalità di quest'ultima[53]».

Per quanto attiene all'idoneità della direttiva a salvaguardare la pubblica sicurezza, la Corte precisa come ammettere la possibilità per le autorità pubbliche di accedere a tali dati costituisca, sicuramente, una misura che consente una migliore prevenzione e repressione dei reati. Tuttavia, tale considerazione non è risolutiva circa la questione della proporzionalità della disciplina contenuta nella direttiva 24/2006/CE. Infatti, rimane impregiudicato il tema riguardante la sua necessità. Dato il contesto in cui la citata normativa opera, il canone della necessità della compressione dei diritti dei singoli è da interpretarsi in senso restrittivo, richiedendo, quindi, di verificare se risultino rispettati i limiti alla potestà legislativa.

Più in particolare, i confini dell'attività legislativa sono da ricercarsi nell'esistenza di regole precise in grado di delimitare compiutamente l'àmbito applicativo della direttiva. Non solo, deve essere garantito alle persone che subiscono la conservazione dei loro dati di navigazione, un livello alto di sicurezza contro eventuali abusi da parte del potere pubblico o contro utilizzazioni illecite dei dati raccolti. L'applicazione di tale griglia alla direttiva ne fa emergere la sua sproporzionalità. In primo luogo, i dati cui dovrebbe applicarsi la disciplina in commento sono quelli estratti da tutti i mezzi di comunicazione usati da tutti i cittadini

[53] Cfr. ECLI:EU:C:2014:238, § 47.

dell'Unione europea, senza che sia posta alcuna distinzione in ordine ai diversi tipi di informazioni che possono essere ottenute. In secondo luogo, la direttiva, pensata per finalità afferenti alle indagini penali, si applica ai dati riguardanti anche i cittadini che non sono né indagati né collegati, anche in via indiretta, con la commissione di un reato. In terzo luogo, manca qualsiasi disposizione che vada ad arginare il potere di accesso e di successivo utilizzo di tali dati da parte delle autorità nazionali. In particolare, non viene previsto nessun potere di controllo da parte di un giudice o di un'autorità amministrativa indipendente sulla legittimità dell'accesso e dell'uso delle informazioni registrate dagli operatori telefonici e dai fornitori di connettività.

La conseguenza del discorso condotto dalla Corte è stata quella di ritenere la direttiva 24/2006/CE costitutiva di un'ingerenza non giustificata nei diritti fondamentali protetti dagli artt. 7, 8 Carta di Nizza[54].

La dottrina dal canto suo non ha mancato di apprezzare la strada intrapresa dalla Corte di giustizia dell'Unione europea attraverso la sentenza citata. Infatti è stato sottolineato come la Corte si sia preoccupata di garantire i diritti fondamentali dei cittadini europei, senza che tale impostazione vieti completamente l'utilizzo dei più sofisticati mezzi di indagine[55]. Tale risultato è stato raggiunto attraverso la creazione di una sorta di *vademecum* contenente le garanzie minime che devono essere rispettate in materia di *data retention*.

[54] Grazie ad una recentissima pronuncia, l'orientamento citato è stato riconfermato dalla Corte di Giustizia, che ha ribadito come sia contraria al diritto dell'Unione Europea una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente. Cfr. ECLI:EU:C:2016:970.

[55] Si esprime in tal senso 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?*, in *Dir. pen. cont.*, 2014, n. 4, p. 187.

Tuttavia, la sentenza della Corte porta con sé anche numerose questioni. La prima, di carattere generale, riguarda la validità delle singole normative nazionali[56]. Volgendo un rapido squadro al nostro Paese, sembrerebbe emergere il contrasto tra la normativa italiana in tema di *data retention* e la citata sentenza delle Corte di Giustizia dell'Unione europea. Infatti l'art. 132 Codice *privacy* impone ai fornitori di servizi di telecomunicazioni l'obbligo di conservare i dati esterni delle comunicazioni telefoniche per ben ventiquattro mesi e quelli riguardanti le comunicazioni telematiche per dodici mesi[57]. Questi sono i termini entro i quali il pubblico ministero può, con un proprio decreto, richiedere l'acquisizione dei dati relativi alle comunicazioni effettuate dall'indagato, dalla persona offesa o dalle parti private. Simmetricamente, un potere simile è stato anche affidato al difensore dell'indagato, il quale può richiedere tali dati nelle forme dell'art. 391 – *quater* c.p.p. La disciplina citata non prevede nessuna individuazione dei reati che possono legittimare l'acquisizione dei dati relativi alle comunicazioni e nessuna forma di controllo sulle scelte del pubblico ministero. Inoltre, non sono previsti particolari obblighi in relazione alla predisposizione di elevate misure di sicurezza per proteggere i dati in oggetto.

Secondo la dottrina, quelle citate sarebbero le maggiori criticità da correggere da parte del legislatore[58]. Infatti, proseguono questi studiosi, in un'ottica di modifica legislativa,

[56] Cfr. R. FLOR, *op. cit.*, p. 187. La sentenza è stata emanata sulla base del meccanismo del rinvio pregiudiziale di cui all'art. 267 T.F.U.E., per cui, sicuramente, la pronuncia ha valore vincolante per il giudice *a quo* che ha sollevato la questione circa la legittimità della direttiva 2006/24/CE in relazione ai trattati dell'Unione europea. Inoltre, l'interpretazione che la Corte di Lussemburgo dà delle norme comunitarie è anch'essa vincolante e comporta l'invalidità della direttiva impugnata. Il vero punto controverso è l'efficacia delle normative nazionali emanate sulla base della citata direttiva. Al momento, nessun pare aver ipotizzato un'invalidità "a cascata", tuttavia, rimane sempre il potere-dovere per i giudici nazionali di poter utilizzare lo strumento dell'art. 267 T.F.U.E. per far emergere eventuali profili di contrasto tra la normativa nazionale e i trattati dell'Unione europea. Sul punto, per ulteriori considerazioni si rimanda a E. COLOMBO, *"*Data Retention*" e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen.*, 2014, pp. 2711 ss. Per quanto riguarda la validità dell'art. 132 Codice *privacy*, v. *infra* nel testo.

[57] Per ulteriori considerazioni in relazione all'acquisizione dei dati di traffico telematico *ex* art. 132 Codice *privacy* v. Cap. IV, § 4.

[58] In tal senso, v. R. FLOR, *op. cit.*, p. 190.

si potrebbe pensare ad un sistema in cui il pubblico ministero richieda al giudice per le indagini preliminari l'autorizzazione all'acquisizione dei dati delle comunicazioni intervenute tra determinati soggetti. Quest'ultimo sarebbe incaricato di controllare sia il *fumus commissi delicti* riguardante solamente certe fattispecie di reato sia il rispetto delle opportune misure di carattere tecnico che vadano a garantire la genuinità dei dati così ottenuti. Tuttavia, tale soluzione, seppur valida per il nostro ordinamento, sembrerebbe quella meno opportuna in una prospettiva di maggior respiro. Infatti, alla luce anche della dimensione transnazionale di molte fattispecie di reato, sarebbe più opportuno un intervento a livello europeo che possa garantire non solo l'uniformità delle legislazioni dei paesi dell'Unione ma anche la tutela dei diritti fondamentali dei cittadini europei[59].

Chiariti i rapporti, non privi di aspetti di continuità, tra la normativa italiana e la pronuncia della Corte di Giustizia in tema di *data retention*, permane il quesito circa la validità dell'art. 132 Codice *privacy*. Sul punto non sono mancate soluzioni diverse. Secondo alcuni, la contrarietà del diritto interno al diritto UE non potrebbe che essere risolta alla luce del principio di supremazia di quest'ultimo rispetto al primo. Non essendo possibile un'interpretazione conforme della normativa italiana alla sentenza in commento, ne risulterebbe un obbligo per il giudice di disapplicare l'art. 132 Codice *privacy* e di dichiarare inutilizzabile la prova così ottenuta[60]. In una posizione più sfumata si pone, invece, chi ammette la possibilità per il giudice di poter effettuare un rinvio pregiudiziale alla stessa Corte di Giustizia a norma dell'art. 267 TFUE.

[59] Ancora, R. FLOR, *op. cit.*, p. 190.

[60] Posizione espressa da F. IOVENE, Data retention *tra passato e futuro. Ma quale presente?*, in *Cass. pen.*, 2014, pp. 4281 s.

3. (segue): dalla tutela della vita privata nella Convenzione europea dei diritti dell'uomo alla delimitazione della riservatezza informatica

La Convenzione europea dei diritti dell'uomo, di cui è stato precedentemente tratteggiato il valore da attribuirle all'interno delle fonti dell'ordinamento italiano, si occupa della tutela da accordare alla vita privata nell'art. 8, § 1 C.e.d.u., il quale stabilisce che «ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza». La formulazione della disposizione riprende, anche se con diverse sfumature, l'art. 12 della Dichiarazione universale dei diritti umani[61].

Seppur riconosciuto come la base per la tutela di numerosi diritti, l'art. 8 § 1 C.e.d.u. ha il suo nucleo fondamentale nell'offrire protezione al c.d. *right to be let alone*, ossia al diritto di ciascun individuo di vivere liberamente senza alcuna interferenza da parte dello Stato o di altri privati individui.

Gli articoli della Convenzione europea dei diritti dell'uomo non possono essere studiati senza fare riferimento all'interpretazione che degli stessi ne dà la Corte europea dei diritti dell'uomo. Ai fini del presente lavoro, l'analisi della sua giurisprudenza sarà condotta con l'obiettivo di individuare da un lato, quel nucleo di situazioni soggettive protette dalla Convenzione e, dall'altro, a precisare le eventuali modalità con cui lo Stato può limitare tali diritti. In questo contesto, risulta necessaria un'ulteriore premessa: alla luce delle differenti tradizioni giuridiche dei Paesi membri del Consiglio d'Europa, la Corte europea, nell'individuazione delle situazioni soggettive protette dalla C.e.d.u., si preoccupa di ricercare nozioni

[61] La dichiarazione universale dei diritti umani è stata proclamata dall'Assemblea Generale dell'Organizzazione delle Nazioni Unite il 10 dicembre 1948. L'art. 12 D.u.d.u. si caratterizza per essere, sotto certi aspetti, più generale rispetto all'art. 8 C.e.d.u. Infatti, solo il primo menziona tra i beni tutelati l'onore e la reputazione. Tuttavia, l'art. 8 C.e.d.u. contiene una più puntuale elencazione delle possibili restrizioni che i diritti garantiti possono sopportare.

indipendenti e sufficientemente elastiche da poter essere trasportate in tutti gli ordinamenti dei singoli Stati[62].

Tra i molteplici profili che vengono in gioco, il primo risulta essere sicuramente quello riguardante la nozione di vita privata fatta propria dalla Convenzione così come interpretata dai giudici di Strasburgo. Si tratta di un concetto estremamente ampio e di difficile delimitazione in via astratta e definitiva. Questa indefinitezza ha portato taluni a rilevare come questa sia una fattispecie espressamente pensata come una sorta di clausola generale per offrire tutela a tutte quelle situazioni soggettive che non sono espressamente previste dall'art. 8, § 1 C.e.d.u.[63]. Ciò in quanto l'obiettivo della Convenzione europea dei diritti dell'uomo è quello di tutelare la persona in quanto tale e di offrirle una protezione a tutto tondo. Proseguendo nel ragionamento, si può affermare che tutte le volte in cui vi sarebbe una violazione di certi rapporti o relazioni afferenti al singolo inteso come individuo, ma che non siano direttamente tutelate dall'art. 8, § 1 C.e.d.u., sarebbe proprio la clausola della tutela della vita privata ad offrire un idoneo strumento di garanzia per la Corte e.d.u.[64]. In quest'ottica, si colloca la giurisprudenza della Corte europea dei diritti dell'uomo, la quale ricomprende nella definizione di vita privata un gran numero di situazioni differenti.

Per comprendere l'approccio fatto proprio dai giudici di Strasburgo, risulta utile fare riferimento ad una ormai risalente pronuncia nella quale la Corte ha offerto una definizione molto ampia di vita privata[65]. Il fatto da cui origina la pronuncia può essere così brevemente

[62] Per alcune considerazioni sull'utilizzo del c.d. margine di apprezzamento da parte della Corte europea dei diritti dell'uomo, cfr. *supra* § 1.

[63] Cfr. S. FÙRFARO, *Il diritto alla riservatezza*, cit., p. 34; nel medesimo senso, v. anche M. MURGO, *Il diritto al rispetto della vita privata*, in *La CEDU e il ruolo delle Corti*, a cura di P. Gianniti, Zanichelli, Bologna, 2015, p. 1156.

[64] Ancora, S. FÙRFARO, *op. cit.*, p. 34.

[65] Si fa riferimento a Corte eur., 28 gennaio 2003, Peck c. Regno Unito. Tutte le sentenze della Corte citate possono essere reperite sul sito ufficiale della stessa, all'indirizzo http://hudoc.echr.coe.int/.

riassunto: un cittadino inglese tenta il suicidio in un luogo pubblico; ciò che accade immediatamente dopo il tentativo viene ripreso dalle telecamere a circuito chiuso del comune in cui si sono svolti i fatti e viene diffuso tramite i media nazionali in tutto il Regno Unito. Il ricorrente ritiene che una tale diffusione del filmato contrasti con il suo diritto ad una vita privata. Il *punctum dolens* riguarda la possibilità di propagazione indeterminata del video in questione. Infatti, non viene posto in dubbio il diritto dell'autorità di riprendere comportamenti avvenuti in pubblico per finalità di sicurezza, ma la possibilità che tali riprese possano essere diffuse in tutto il Paese attraverso i media. In altri termini, il ricorrente afferma di aver accettato la possibilità che qualcuno lo vedesse tentare il suicidio, ma che non avrebbe potuto prevedere che quel video si sarebbe poi diffuso in tutta la nazione[66]. In senso opposto, il governo del Regno Unito rileva come i comportamenti del ricorrente siano stati posti in essere nella pubblica strada. Ne consegue che, vi sarebbe una sorta di rinuncia dello stesso a qualsiasi pretesa di riservatezza[67].

La Corte europea dà ragione al ricorrente proprio sulla base dell'ampiezza riconosciuta al diritto alla vita privata. Infatti anche se tale nozione non è facilmente definibile a priori, tuttavia, una corretta analisi della *ratio* della tutela accordata a questo bene giuridico può aiutare l'interprete. In particolare, i giudici di Strasburgo sottolineano come il ricorrente non avesse rinunciato a qualsiasi tipo di protezione circa la riservatezza dei suoi atti. Ciò in quanto egli da un lato, non stava partecipando ad una manifestazione pubblica e, dall'altro, non è un personaggio pubblico. Inoltre, sicuramente il ricorrente, tentando il suicidio in un luogo pubblico, aveva accettato che qualche passante o che le forze di sicurezza potessero vederlo. Tuttavia, non aveva in alcun modo previsto la possibilità che il suo comportamento

[66] Cfr. Corte eur., 28 gennaio 2003, Peck c. Regno Unito, § 55.

[67] Cfr. Corte eur., 28 gennaio 2003, Peck c. Regno Unito, § 53.

potesse essere visto da un numero di persone così ampio qual è quello degli spettatori dei diversi mezzi di comunicazione che avevano appreso e rilanciato il video. In altri termini, sottolinea il giudice europeo, la semplice commissione di un determinato fatto in un luogo pubblico non esclude il diritto di ciascuno a mantenere un livello seppur minimo di riservatezza. Tale diritto, infatti, segue l'individuo in ogni sua azione o comportamento indipendentemente dal luogo in cui egli agisce; l'unica differenza riguarda la latitudine delle sue aspettative legittime[68].

Sempre al fine di dar conto dell'estensione del termine vita privata nel linguaggio della C.e.d.u., merita di essere citata, almeno, un'altra pronuncia della Corte europea dei diritti dell'uomo. In tale decisione, una delle questioni affrontate riguardava la legittimità di una registrazione compiuta da Scotland Yard all'insaputa del dichiarante per finalità di repressione dei reati[69]. In particolare, i ricorrenti lamentavano la lesione del proprio diritto alla riservatezza in quanto non era possibile immaginare che le conversazioni avute tra loro e la polizia potessero essere registrate. Proprio quest'ultima circostanza di fatto è stata sottolineata dai giudici di Strasburgo al fine di sostenere la riconducibilità dell'accaduto alla fattispecie delineata dall'art. 8, § 1 C.e.d.u. Infatti, se da un lato, sicuramente il livello di tutela cambia a seconda del luogo in cui si attua un determinato comportamento, per cui nel momento in cui taluno si espone sulla pubblica via perde parte del diritto alla vita privata; dall'altro lato, il medesimo diritto rientra in gioco allorché quei comportamenti o quelle dichiarazioni, che possono essere liberamente visti o ascoltati da chiunque, siano registrati e catalogati da parte dell'autorità. In questo caso, l'utilizzo dello strumento tecnico permette di

[68] Cfr. Corte eur., 28 gennaio 2003, Peck c. Regno Unito, § 62. Sulla stessa linea argomentativa si potrebbe fare riferimento ad un diritto alla riservatezza *online* che segue il soggetto durante tutta la sua attività in rete.

[69] Cfr. Corte eur. 25 settembre 2001, P.G. e J.H. c. Gran Bretagna.

ottenere delle informazioni che non possono non essere qualificate come personali e, quindi, risultano assistite dalla tutela dell'art. 8, § 1 C.e.d.u.[70].

Cercando di riprendere le fila del complesso discorso fin qui condotto in relazione alla riservatezza, merita di essere citato quell'orientamento dottrinale che, partendo dalle disposizioni normative citate, giunge a riconoscere l'esistenza di un diritto alla riservatezza informatica[71]. Il punto di partenza del ragionamento è costituito dalla promiscuità dei dati contenuti in un elaboratore elettronico: questo, infatti, non solo è in grado di memorizzare informazioni di per sé sensibili – come potrebbe essere un diario privato – ma, inoltre, può immagazzinare una serie di dati – come i metadati cui si è fatto riferimento nel paragrafo precedente – che combinati tra di loro possono fornire rilevanti informazioni circa l'utilizzatore del *device*[72]. In questo contesto, come si avrà modo di specificare meglio più avanti, anche la tutela del c.d. domicilio informatico risulta insufficiente[73]. Soltanto l'idea di una protezione dei dati informatici in quanto tali sembrerebbe in grado di offrire una effettiva salvaguardia a quello spazio privato che costituisce il nucleo fondamentale del diritto alla riservatezza.

Per questo motivo, può essere utile una lettura combinata non solo della Costituzione ma anche della C.e.d.u. e della Carta di Nizza. L'art. 2 Cost. offre, come visto precedentemente, un primo appiglio per il riconoscimento del diritto alla riservatezza nel nostro ordinamento. Tuttavia, non è in grado di regolare i conflitti che possono sorgere tra le esigenze di *privacy* dei soggetti coinvolti in un'indagine penale e le necessità proprie di quest'ultima[74]. In questo

[70] Cfr. Corte eur. 25 settembre 2001, P.G. e J.H. c. Gran Bretagna, § 57.

[71] Si fa riferimento a F. IOVENE, *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont.*, 2014, nn. 3-4, pp. 334 ss.

[72] Cfr., F. IOVENE, *Le c.d. perquisizioni*, cit., p. 334.

[73] Sul tema, si rimanda alle considerazioni svolte *infra* nel § 3.

[74] V., C. MARINELLI, *op. cit.*, p. 88.

contesto entrano in gioco le carte dei diritti approvate in àmbito europeo, le quali, come chiarito, hanno rilevanza nel nostro ordinamento[75]. Queste permettono di integrare l'art. 2 Cost. in tema di riservatezza, seguendo uno schema di ragionamento già fatto proprio dalla Corte costituzionale[76], in modo da offrire un possibile bilanciamento dei beni giuridici in gioco. In quest'ottica, richiamando la giurisprudenza citata tanto dei giudici di Strasburgo quanto di quelli del Lussemburgo, può arrivare ad affermarsi che gli atti investigativi che vanno a comprimere il diritto alla vita privata di cui agli artt. 8 C.e.d.u. e 7 Carta di Nizza possono dirsi legittimi soltanto se dotati di un'adeguata base giuridica, sottoposti ad un controllo di carattere giurisdizionale e rispettosi del principio di proporzionalità[77].

[75] Sul valore da attribuire alla C.e.d.u. e alla Carta di Nizza, v. *supra* § 1.

[76] V., *supra*, § 1. A favore di tale integrazione, seppur in riferimento alla riservatezza intesa in senso generico, si esprimeva F. BRICOLA, *op. cit.*, pp. 1097 ss.

[77] Cfr. F. IOVENE, *Le c.d. indagini*, cit., p. 338.

4. L'evoluzione del concetto di domicilio accettato nella Costituzione e nella Convenzione europea dei diritti dell'uomo

L'art. 14 Cost. sancisce *per tabulas* l'inviolabilità del domicilio. Le ragioni che hanno animato i costituenti in questa scelta sono state molteplici. In prima battuta, vi è stata la considerazione della necessità per l'uomo di potersi legittimamente isolare dal resto della società senza che un tale comportamento potesse essere causa di alcun pregiudizio verso lo stesso. Più nello specifico, l'obiettivo che si voleva raggiungere era quello di arginare il potere di intrusione nelle mura domestiche da parte dell'autorità pubblica, al fine di garantire uno spazio di riservatezza per ciascuno. Spazio da intendersi, almeno da un punto di vista storico, come luogo fisico all'interno del quale l'autorità non può entrare e nel quale il singolo persegue liberamente i propri interessi di carattere non solo affettivo, ma anche lavorativo o spirituale[78]. Come viene ammesso da alcuni, il domicilio diviene quell'ambiente all'interno del quale ciascuno può «agi[re] con una libertà di comportamento che spesso può ignorare i limiti delle norme di convivenza[79]». In seconda battuta, la tutela del domicilio ha un effetto indiretto estremamente importante per quanto attiene alla garanzia di altri diritti fondamentali. Questi, infatti, non solo offre copertura costituzionale a diritti, come quello alla riserva-

[78] La matrice storica della tutela del domicilio è da ritrovare nella protezione del diritto di proprietà: l'intimità veniva protetta in quanto fosse esplicata nella propria abitazione, mentre, altri luoghi, come gli alberghi o le locande, non godevano di una tale protezione rispetto ai poteri pubblici. Per ulteriori chiarimenti sul punto, si rimanda alle considerazioni di G. AMATO, sub *art. 14*, in *Commentario della Costituzione. Rapporti civili*, a cura di G. Branca, Zanichelli, Bologna, 1977, pp. 54 s.; R. CHIARELLI, *Domicilio I) libertà di domicilio*, in *Enc. giur. Treccani*, Roma, 1989, pp. 1 s.

[79] Cfr. I FASO, *La libertà di domicilio*, Giuffrè, Milano, 1968, p. 82. Inoltre, A. PACE, *Problematica delle libertà costituzionali. Lezioni. Parte speciale*, Cedam, Padova, 2° ed., 1992, p. 213 rileva come l'inviolabilità del domicilio ha l'effetto di rendere leciti comportamenti che se fossero compiuti sulla pubblica via potrebbero costituire reato.

tezza, non codificati dal costituente; ma inoltre, permette il rafforzamento di situazioni soggettive già protette dalla Costituzione[80]. Con quest'ultima affermazione ci si riferisce alla tutela delle libertà di associazione, di culto, di insegnamento, di iniziativa economica, di organizzazione politica e sindacale. Infatti la previsione di una tutela rafforzata del domicilio rende queste libertà concrete limitando il potere di intervento dell'autorità pubblica[81].

Nel quadro ideologico sommariamente descritto si inserisce la discussione tenutasi in Assemblea Costituente, nella quale, proprio in ragione di quanto è stato affermato, la tutela del domicilio è sempre stata vista come strettamente collegata a quella della libertà personale[82]. A riprova di tale affermazione vi sarebbe la prima formulazione dell'art. 8 del progetto di Costituzione presentato alla Prima Sottocommissione, nel quale si tutelavano, attraverso la medesima disposizione, sia il domicilio sia la libertà personale. Solo in un secondo momento si decise di dedicare un'apposita disposizione al tema del domicilio.

Già dalla discussione registratasi in senso alla Prima Sottocommissione parrebbe implicitamente emergere l'idea di superare ed ampliare la garanzia del domicilio così come formulata in epoca pre-costituzionale. Infatti allorché si discusse circa la creazione di un «privilegio» a favore della sola abitazione privata rispetto alle sedi di società, partiti o associazioni, la scelta fu quella di non effettuare alcuna distinzione in ordine ai domicili da proteggere[83]. Il risultato di tale opzione è stato quello di ammettere una tutela generalizzata di

[80] In tal senso si esprimeva, P. BARILE, *Diritti dell'uomo e libertà fondamentali*, Società editrice il Mulino, Bologna, 1984, p. 154.

[81] A. PACE, *Problematica*, cit., p. 213.

[82] Come sottolineato da P. CARETTI, *Domicilio (libertà di)* in *Dig. discipl. pubbl.*, Giuffrè, Milano, 1990, vol. V, p. 321 il dibattito in sede di Assemblea Costituente ebbe come punto di partenza tre elementi: la libertà di domicilio come proiezione della libertà personale; l'equiparazione tra domicilio e privata dimora; la necessità di distinguere tra interferenze pubbliche e private nel godimento del domicilio.

[83] L'on. Basso nella seduta del 10 aprile 1947 riconosce esplicitamente l'importanza di «difendere [non] soltanto l'abitazione, ma anche, per esempio, l'azienda, la sede di un partito o di un'associazione». A sostegno di tale posizione vi sarebbe sia la volontà di offrire una garanzia completa, che copra tutti gli aspetti della personalità umana sia la consapevolezza degli effetti irrazionali che potrebbero derivare da un "privilegio" a favore dell'abitazione:

tutti i luoghi in cui si manifestava la personalità del singolo. In tal modo, da un lato, si prevedeva una nozione diversa rispetto a quella di cui all'art. 43 c.c. e, dall'altro, si faceva riferimento ad un concetto più ampio di quello elaborato dalla dottrina e dalla giurisprudenza in relazione all'art. 614 c.p.[84].

La *ratio* sottesa alla scelta di un concetto di domicilio di tale ampiezza è da ricercare nella già accennata connessione tra libertà personale e inviolabilità di quest'ultimo. L'obiettivo che i Costituenti volevano raggiungere era quello di permettere la piena manifestazione della personalità dell'individuo all'interno dei luoghi da questo abitati. In questa direzione, sembrava quasi ovvia l'idea per cui la tutela della sola «privata dimora», cui fa riferimento il codice penale, non sarebbe stata sufficiente a garantire la piena esplicazione della personalità del singolo. Questa, infatti, si manifesta, oltre che tra le mura domestiche, anche in altri contesti quali le sedi di partiti o di associazioni, le aziende, gli studi professionali.

Partendo da queste premesse, i Costituenti circondarono la tutela dell'inviolabilità del domicilio di due garanzie: la riserva di legge e quella di giurisdizione. Entrambe, almeno in prima battuta, hanno come obiettivo quello di evitare ingerenze da parte dell'esecutivo nella vita privata dei cittadini[85].

Tuttavia, indipendentemente dal dibattito svoltosi in Assemblea Costituente, deve essere affrontata la questione circa l'esatta delimitazione del concetto di domicilio fatto proprio dalla Costituzione. Infatti, come rilevato dalla dottrina, il termine, da un lato, non designa

---

chi volesse sottrarre dei documenti all'autorità potrebbe semplicemente trasferirli nella propria abitazione, rendendo, nella pratica, inutile qualsiasi differenziazione tra privata dimora e altri luoghi. Si rimanda sul punto alle considerazioni di G. AMATO, *op. cit.*, pp. 56 s.

[84] Cfr. P. CARETTI, *op. cit.*, p. 322.

[85] Ovviamente, la logica seguita dal Costituente è stata quella dell'equo bilanciamento tra i diritti dei singoli e quelli della collettività: fin dalla discussione in Assemblea si ammetteva la necessità di disegnare una garanzia che non fosse assoluta, ma che permettesse all'autorità di violare il domicilio qualora vi fossero esigenze di sanità o di incolumità pubblica. Cfr. G. AMATO, *op. cit.*, p. 57.

alcuna realtà del mondo sensibile, essendo un concetto prettamente giuridico; dall'altro, è presente nel nostro ordinamento con riferimento ad almeno due situazioni di fatto estremamente diverse[86]. L'unione di queste due considerazioni ha reso necessario un intervento definitorio da parte degli studiosi.

Sicuramente, dato che i Costituenti avevano ben presente le disposizioni vigenti al momento della redazione della Carta costituzionale, un primo tentativo di chiarificare il significato del termine domicilio non può non assumere come punto di partenza proprio la normativa pre-costituzionale. In quest'ottica, un possibile referente potrebbe essere individuato nell'art. 43, co. 1° c.c., che contiene una definizione di domicilio come di quel «luogo in cui [la persona] ha stabilito la sede principale dei suoi affari e interessi». Nonostante tale opzione sia stata accolta in una risalente pronuncia da parte della Corte costituzionale, l'identificazione tra il domicilio di cui al diritto civile e quello fatto proprio dalla Costituzione risulterebbe infondata[87]. Infatti, anche ad una sommaria lettura, sembrerebbe chiara la diversa prospettiva accolta dalla Costituzione e dal codice civile. Quest'ultima, infatti, si preoccupa di localizzare geograficamente la persona per motivi prettamente ancorati alla certezza degli scambi tra le persone[88]. Il codice civile non intende il domicilio come spazio in cui viene a disvelarsi la vita privata di un individuo quanto, piuttosto, come luogo fisico in cui taluno svolge la propria attività economica[89]. L'idea stessa di garantire una qualche forma di inviolabilità al domicilio-recapito parrebbe incongruente. La prospettiva accolta dal codice civile non potrebbe essere più distante rispetto a quella della Costituzione, nella quale, come già

[86] Così, C. E. TRAVERSO, *Il concetto di domicilio*, in *Studi in onore di Antonio Amorth*, Giuffrè, Milano, vol. II, p. 589.

[87] Ci si riferisce a Corte cost., 24 aprile 1975, n. 106 in *Giur. cost.*, 1975, pp. 1203 ss.

[88] Tra i tanti, v. P. VERONESI, *Per un'interpretazione costituzionale del concetto di "domicilio"*, in *Ann. univ. Ferrara*, 2003, pp. 110 s.

[89] Più ampiamente sul punto, v. C. E. TRAVERSO, *op. cit.*, pp. 597 ss.

chiarito, l'inviolabilità del domicilio è concepita come strumentale a garantire l'effettiva tutela della libertà personale. Se la Costituzione sembra porre al centro le esigenze di tutela della personalità del singolo, il codice civile, viceversa, si preoccupa di individuare un luogo al fine di garantire la certezza dei rapporti giuridici di diritto privato.

Escluso qualsiasi richiamo all'art. 43 c.c., altro referente normativo possibile potrebbe essere l'art. 614 c.p. che punisce la violazione di domicilio. Secondo una parte della dottrina, questa disposizione costituirebbe il presupposto della norma costituzionale[90]. La linea argomentativa tesa a supportare tale statuizione procede tendenzialmente per esclusione. Il punto di partenza è dato dal fatto che la Costituzione non fornisce in alcuna disposizione una definizione del concetto di domicilio. Nemmeno una lettura sistematica delle norme potrebbe aiutare l'interprete in tale opera. Stando così le cose, sembrerebbe che il Costituente abbia voluto richiamarsi ad istituti e definizioni propri della tradizione giuridica precedente alla Costituzione. Tra queste, scartata la rilevanza, per le ragioni già indicate, delle disposizioni sul domicilio del codice civile o delle leggi in materia fiscale, il discorso andrebbe necessariamente a parare sul concetto penalistico di domicilio. Questo per almeno due ragioni: la prima, di carattere storico, è data dal fatto che l'art. 14 Cost. si inscrive in una tradizione normativa che, partendo dall'art. 27 dello Statuto albertino, ha sempre avuto come riferimento la disposizione penalistica. La seconda pone in luce l'identità di *ratio* sottesa ad entrambe le disposizioni: queste, infatti, intendono tutelare la libertà personale attraverso la protezione dei luoghi in cui questa si esplica.

[90] Tesi sostenuta fatta propria, tra gli altri, da P. BARILE – E. CHELI, *Domicilio (libertà di)*, in *Enc. dir.*, Giuffrè, Milano, 1964, vol. XIII, p. 862; P. BARILE, *Le libertà nella Costituzione. Lezioni*, Cedam, Padova, 1966, p. 149; F. PAZIENZA, *Domicilio IV) delitti contro la inviolabilità del domicilio*, in *Enc. giur. Treccani*, 1989, pp. 1 s.; M. SINISCALCO, *Domicilio (violazione di)*, in *Enc. dir*, Giuffrè, Milano, 1964, Vol. XIII, p. 873.

Da ultimo, un'altra parte della dottrina sostiene l'idea per cui la Costituzione accoglierebbe un concetto autonomo di domicilio, il quale sarebbe ben più ampio di quello rintracciabile nelle norme di legge ordinaria. Infatti l'art. 14 Cost. tutelerebbe qualsiasi spazio in cui si esplica la personalità del soggetto: il domicilio costituirebbe «la proiezione spaziale della persona[91]». Sosterebbero questa impostazione argomentazioni di vario tipo. La prima è di carattere sistematico. In questo senso si rileva come l'art. 14 Cost. si colloca fra le norme che si occupano dei rapporti tra individuo e Stato e, più precisamente, tra quelle che tendono a garantire la libertà personale. Pertanto, mentre il codice penale avrebbe come obiettivo la c.d. *pax domestica*, la Costituzione si porrebbe nell'ottica, più ampia e generale, della tutela della libertà del singolo contro ingerenze sia da parte di privati sia da parte dello Stato. Non solo: considerando che violazioni del domicilio, intese come raccolta di informazioni di carattere riservato che possono limitare la piena esplicazione della libertà individuale, possono essere compiute anche senza introdursi effettivamente nello stesso, sembrerebbe più aderente allo spirito della Costituzione pensare al domicilio come al rapporto tra un individuo e il luogo in cui questi manifesti in maniera riservata la propria personalità. In altri termini, il concetto costituzionale di domicilio sarebbe più ampio di quello ammesso dal codice penale.

In proposito occorre aggiungere come altri abbiano sottolineato come la relazione tra l'art. 14 Cost. e l'art. 614 c.p. sia più complessa[92]. Infatti, se da un lato, sicuramente, la disposizione costituzionale ha ripreso un concetto proprio della scienza penalista degli anni '30 del '900, dall'altro lato, il medesimo articolo è servito come base per giungere ad un'interpretazione più ampia del concetto di domicilio. La relazione tra le due norme sarebbe biunivoca:

[91] La definizione è stata coniata da A. AMORTH, *La Costituzione italiana. Commento sistematico*, Giuffrè, Milano, 1948, p. 62.

[92] Cfr. P. VERONESI, *op. cit.*, pp. 113 s.

non solo la ricostruzione del domicilio "costituzionale" avrebbe effetti sulla delimitazione dell'àmbito applicativo dell'art. 614 c.p. ma, inoltre, l'applicazione concreta della disposizione del codice penale potrebbe aiutare l'interprete a disegnare una più compiuta nozione di domicilio.

Dal canto suo, la giurisprudenza ordinaria si è orientata verso un'interpretazione molto ampia del concetto di privata dimora di cui all'art. 614 c.p., andando sostanzialmente a sovrapporre la disposizione penalistica con quella dell'art. 14 Cost. Sul punto, è opportuno effettuare una prima distinzione, tra i beni immobili e quelli mobili. Mentre per i primi la Corte di cassazione ne riconosce pacificamente la natura di domicilio; diverso è il discorso per i secondi. In questo caso, diventa necessario analizzare la fattispecie concreta sottoposta all'attenzione del giudice: non tutti i beni mobili sono suscettibili di diventare domicilio, ma solo quelli stabilmente utilizzati come abitazione dalla persona. Per cui, potrebbero essere considerati domicilio anche la tenda o l'automobile allorché essi siano effettivamente utilizzati come luogo di privata dimora[93]. La linea generale della giurisprudenza di legittimità sembrerebbe essere quella di andare a verificare caso per caso se l'attività svolta dal soggetto nello spazio considerato costituisca un effettivo dispiegamento della sua personalità[94]. Nel medesimo senso si è orientata anche la giurisprudenza costituzionale. Infatti escludendo il già citato isolato arresto giurisprudenziale in cui si parificava il domicilio civilistico a quello costituzionale, la Corte costituzionale ha sempre analizzato la garanzia dell'inviolabilità del

[93] Cfr. Cass. sez. VII, 12 gennaio 2015, Colombo, in *C.e.d. cass.* n. 263188, la quale ha riconosciuto, proprio in ragione delle attività espletate in un camper, natura di privata dimora anche a quest'ultimo. Diverso il discorso per quanto riguarda le autovetture, seppur riconosciute come idonee ad integrare il concetto di domicilio da Cass. sez. II, 12 marzo 1998, Zagaria, in *C.e.d. cass.* n. 211142, tale pronuncia è rimasta isolata. Infatti, la giurisprudenza maggioritaria, pur condividendo l'assunto per cui teoricamente un'automobile possa diventare un luogo di privata dimora, generalmente non riconosce alla stessa il valore di domicilio. V., *ex multis*, Cass. sez. IV, 14 marzo 2013, Todero, in *C.e.d. cass.* n. 255894. In dottrina, v. A. PACE, *Problematica*, cit., p. 215.

[94] V., in tal senso, P. VERONESI, *op. cit.*, p. 117.

domicilio attraverso la lente della tutela della libertà personale del singolo. Questo approccio ha portato a riconoscere come domicilio, tra le altre cose, anche il bagagliaio di un'autovettura[95].

Il tema della garanzia apprestata dalla Costituzione al domicilio è stato oggetto in tempi relativamente recenti di alcune rilevanti pronunce da parte della Corte costituzionale, le quali hanno cercato di chiarire la funzione e la *ratio* dell'art. 14 Cost. Gli arresti giurisprudenziali cui ci si riferisce hanno avuto come punto di riferimento la più volte citata questione della compatibilità con la Costituzione delle videoregistrazioni effettuate all'interno di un domicilio. Nella prima di queste sentenze, i giudici costituzionali ribadiscono espressamente la stretta connessione tra domicilio e libertà personale[96]. Citando direttamente un'autorevole dottrina, la Corte costituzionale sottolinea come la motivazione sottesa alla tutela del domicilio sia quella di «preservare da interferenze esterne comportamenti tenuti in un determinato ambiente[97]». In quest'ottica, la Corte valorizza la valenza essenzialmente negativa della posizione soggettiva riconosciuta dall'art. 14 Cost. In altri termini, il nucleo centrale della disposizione in commento sarebbe rappresentato dal c.d. *ius excludendi*.

In un successivo arresto, la Corte riconosce un ulteriore profilo connesso alla tutela del domicilio, quello della riservatezza[98]. Infatti il contenuto di garanzia dell'art. 14 Cost. è rappresentato non solo dal diritto di decidere chi ammettere o escludere da un determinato

[95] Cfr. Corte cost., 25 marzo 1987, n. 88, in *Giur. cost.*, 1987, pp. 682, nella quale la Corte ha dichiarato l'illegittimità dell'art. 6, co. 2° l. prov. Trento 26 luglio 1973, n. 18 nella parte in cui prevedeva l'intimazione all'apertura anche di mezzi di trasporto che costituiscono luoghi di privata dimora. I giudici costituzionali, dopo aver qualificato il bagagliaio dell'autovettura come domicilio, sottolineano come la Costituzione regoli in maniera restrittiva i poteri di interferenza della privata dimora da parte della pubblica autorità. Sul punto, l'art. 14 Cost. non solo chiarisce la tipologia di atti che possono essere compiuti – ispezioni, perquisizioni e sequestri – ma anche, le finalità di tali atti.

[96] Cfr. Corte. cost., 24 aprile 2002, n. 135, cit.

[97] Cfr. Corte cost., 24 aprile 2002, n. 135, cit., § 2.1

[98] Si fa riferimento a Corte cost., 16 maggio 2008, n. 149, in *Giur. cost.*, 2008, pp. 1825 ss.

luogo, ma anche dal diritto alla riservatezza circa i comportamenti che ivi si compiono. Questa garanzia deriverebbe da un'interpretazione estensiva della disposizione: infatti, se la *ratio* dell'art. 14 Cost. è quella di permettere a ciascun individuo di manifestare liberamente la propria personalità in un determinato ambiente, allora quest'obiettivo può essere pienamente raggiunto evitando che terzi siano in grado di limitare tale potere attraverso comportamenti che, pur non concretizzandosi in un'intrusione di tipo fisico nel domicilio, possano comunque influenzare concretamente la piena esplicazione della vita privata di un individuo[99].

Come rilevato dalla dottrina, quello che emerge dalla lettura della giurisprudenza tanto costituzionale quanto di legittimità è l'importanza della fattispecie concreta, la quale assume un ruolo fondamentale per la individuazione della posizione soggettiva tutelata. Non esisterebbe, in sostanza, una chiara linea di demarcazione tra ciò che può essere considerato domicilio e ciò che non lo è; nel senso che il medesimo luogo potrebbe essere oggetto di tutela a seconda delle vicissitudini del caso concreto[100].

Volendo approfondire maggiormente il contenuto della libertà garantita dall'art. 14 Cost., deve essere rilevato come le vicende relative alla titolarità del bene, attraverso cui si manifesta la personalità del singolo, non sono ininfluenti per la sussistenza o meno della garanzia in discorso. Ciò che si vuole sottolineare è, ancora una volta, la stretta dipendenza tra le contingenze del momento e la sussistenza della tutela. Infatti, come precisato da un'autorevole dottrina, la libertà di domicilio presuppone necessariamente la titolarità di un bene a ciò idoneo[101]. Titolarità che deve essere intesa come situazione concreta di possesso di un

[99] Per quanto attiene alla tutela costituzionale della riservatezza, v. *supra* § 2.

[100] V. in tal senso, P. VERONESI, *op. cit.*, p. 117.

[101] Ci si riferisce a A. PACE, *Problematica*, cit., p. 217.

determinato oggetto che viene utilizzato dall'individuo come domicilio[102]. La libertà di domicilio, in questa lettura, esiste in quanto e fino a quando persiste la situazione di fatto a questa presupposta.

Volendo rivolgere l'attenzione al contesto sovranazionale risulta utile fare riferimento al concetto di domicilio elaborato dalla Corte e.d.u. Dal punto di vista linguistico, il termine domicilio è presente soltanto nella versione francese della Convenzione, viceversa, quella inglese utilizza il più restrittivo termine «*home*». Tuttavia, questa differenza linguistica non è mai stata enfatizzata dalla Corte di Strasburgo, la quale ha riconosciuto come la tutela apprestata dall'art. 8, § 1 C.e.d.u. sia fondamentalmente ispirata a garantire l'individuo contro le interferenze arbitrarie nella propria vita, indipendentemente dalla qualificazione del luogo in cui questa si esplica[103].

Più precisamente, secondo la Corte europea dei diritti dell'uomo il concetto di domicilio designa, innanzitutto, quel luogo in cui si sviluppa la vita privata e familiare. Data l'estesa nozione accettata di vita privata, non deve sorprendere che anche quella di domicilio sia intesa in senso ampio[104]. In questo senso, si può affermare, anzitutto, che il domicilio non è

[102] Secondo A. PACE, *Problematica*, cit., p. 217 anche nel caso in cui taluno spogli violentemente un altro individuo del possesso di un immobile, questi potrebbe comunque invocare la tutela dell'art. 14 Cost. anche contro lo stesso proprietario che ha subìto lo spossessamento.

[103] V., sul punto, Corte eur., 16 dicembre 1992, Niemietz c. Germania, § 30. Parzialmente diverso è il discorso per quanto attiene alla legittimità di quegli strumenti processuali che per le finalità di repressione dei reati vanno a comprimere il diritto alla vita privata. Tra i vari profili attinenti a tale tematica, vi è sicuramente anche quello riguardante il diritto a godere di un proprio spazio privato libero da interferenze da parte dello Stato. In questi casi, però, la Corte europea dopo aver riconosciuto una possibile lesione dell'art. 8, § 1 C.e.d.u. volge il proprio sguardo alla legittimità del comportamento tenuto dallo Stato. Infatti, l'art. 8, § 2 C.e.d.u. ammette la violazione dei diritti sanciti nel primo paragrafo purché questa «sia prevista dalla legge» e costituisca una misura che, «in una società democratica, sia 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». Tuttavia, lo studio dello scrutinio di legittimità in relazione all'art. 8, § 2 C.e.d.u. verrà compiuto più avanti nel prosieguo della trattazione.

[104] Cfr. *supra* § 3.

solo l'abitazione in cui taluno vive, ma ne è ricompresa anche l'area che circonda l'abitazione.

Inoltre, la Corte sottolinea come le interferenze al domicilio sanzionate dalla C.e.d.u. non sono solo quelle concrete, come una perquisizione o l'ingresso non autorizzato di un privato cittadino, ma anche quelle prive di tale fisicità come quelle che passano attraverso la diffusione di un cattivo odore o di un rumore particolarmente molesto[105].

Anche per quanto attiene alla qualificazione di un luogo come domicilio, i giudici di Strasburgo usano un metro di valutazione particolarmente elastico. È, infatti, inteso come tale non solo il luogo in cui una persona già effettivamente vive, ma anche quello verso il quale taluno continua a mantenere legami affettivi[106]. Inoltre, alla luce della considerazione per cui il concetto di domicilio non è delimitato dalle norme dei singoli Stati, ma è, viceversa, una nozione autonoma creata dalla giurisprudenza dei giudici di Strasburgo; ne segue che non può essere definita *home* solo quell'immobile in cui taluno può legittimamente abitare. Secondo la Corte europea dei diritti dell'uomo, il concetto di domicilio emerge dalla sussistenza di alcune circostanze di fatto quali l'esistenza di uno specifico e continuo collegamento tra una persona ed un luogo[107]. Proseguendo in questa direzione, viene riconosciuta la natura di domicilio anche alle residenze secondarie, agli immobili occupati stabilmente pur in assenza di un valido titolo giustificativo, ai caravan[108].

In questo complesso e stratificato quadro teorico si inserisce il concetto di domicilio informatico protetto dal codice penale all'art. 615 *ter*, introdotto con l. 23 dicembre 1993, n.

[105] In tal senso si è espressa Corte eur., 2 novembre 2006, Giacomelli c. Italia, § 76.

[106] Così si è espressa Corte eur., 24 novembre 1986, Gillow c. Regno Unito, § 46.

[107] Cfr. Corte eur. (dec.), 19 settembre 2006, McKay-Kopecka c. Polonia.

[108] V. Corte eur., 31 luglio 2003, Demades c. Turchia, §§ 32-34; Corte eur. Grande Chambre, 18 gennaio 2001, Chapman c. Regno Unito, § 71-74.

547. Dai lavori preparatori della suddetta novella emerge chiaramente come il legislatore abbia voluto richiamarsi direttamente all'art. 14 Cost. come fonte giustificatrice della nuova fattispecie del reato di accesso abusivo ad un sistema informatico[109]. Nell'impostazione del legislatore dei primi anni '90 chiara era l'idea per cui un sistema informatico potesse essere considerato, esattamente come gli altri luoghi via via tutelati dalla giurisprudenza, come area di esplicazione della personalità dell'individuo.

Dal canto suo, la dottrina maggioritaria ha ritenuto corretto il disegno fatto proprio dal legislatore[110]. Tuttavia, all'interno di un generale consenso alle linee portanti dell'intervento legislativo, si palesano due linee argomentative differenti per quanto riguarda l'estensione dell'oggetto del bene giuridico tutelato. Secondo una prima impostazione, ciò che verrebbe tutelato è il sistema informatico in quanto tale; ciò in analogia con quanto avviene con il domicilio fisico[111]. Infatti tanto nel primo quanto nel secondo si tutelerebbe un luogo poiché si presume che in questo vengano svolte attività di carattere personale. La giustificazione della protezione del contenuto del sistema informatico deriverebbe dal fatto stesso che quei dati non sono pubblici, ma conservati all'interno di un dispositivo elettronico[112]. Seguendo questo orientamento si finisce per prescindere da qualsiasi valutazione circa il carattere

[109] Nella relazione di accompagnamento al disegno di legge, viene precisato come «la normativa trova la sua collocazione tra i reati contro l'inviolabilità del domicilio perché i sistemi informatici o telematici, la cui violazione essa reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli artt. 614 e 615 c.p.». M. MURGO, *Diritti*, cit., pp. 770 s., rileva come non sembri così lontana la possibilità che la Corte europea dei diritti dell'uomo riconosca anche la sussistenza del domicilio informatico.

[110] Non sono mancate, tuttavia, alcune voci critiche nei confronti del legislatore. In particolare, F. BERGHELLA – R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, pp. 2330 s. ritenevano inconferente il richiamo all'art. 14 Cost. in quanto «ben di rado si riscontra la presenza di informazioni afferenti a tale sfera squisitamente privata e personale». Tale considerazione risulta essere ormai pacificamente superata dal trascorrere del tempo: la quantità e la qualità dei dati immagazzinati su di un sistema informatico è tale da rendere indiscutibile la necessità di una qualche forma di tutela per tali dati.

[111] Cfr. G. PICA, *Diritto penale delle tecnologie informatiche*, Utet, Torino, 1999, p. 65.

[112] Ancora, G. PICA, *op. cit.*, pp. 64 s.

delle attività compiute nel sistema informatico o dei dati in questo contenuti. Attraverso l'art. 615 *ter* c.p. il legislatore avrebbe consegnato al titolare del sistema informatico uno *ius excludendi* similare a quello che l'individuo può vantare per quanto riguarda il domicilio fisico. Il diritto di escludere taluno dall'utilizzo di un sistema informatico deriverebbe dall'idea per cui all'interno di quest'ultimo vi sarebbe qualcosa di ancor più intimo di quello che potrebbe essere trovato in un domicilio fisico. Infatti vista l'estrema diffusione dell'elettronica di consumo, ormai qualsiasi dispositivo elettronico contiene dati e informazioni personalissime[113]. L'utente consegna al sistema non solo i suoi progetti lavorativi, ma anche i suoi pensieri, i suoi programmi personali per il futuro. Il domicilio informatico, secondo siffatta linea di pensiero, dovrebbe essere inteso come un luogo nel quale l'individuo manifesta la propria personalità, andando così ad aggiungersi agli spazi tradizionali in cui si proietta la soggettività della persona.

Una differente dottrina, accoglie una visuale leggermente differente della questione. Questi studiosi pongono maggiormente l'accento sul dato informatico in quanto tale e sull'immaterialità del luogo informatico, separando il domicilio informatico dal sistema. Punto di partenza della linea argomentativa è la considerazione per cui il domicilio informatico costituirebbe una specificazione di quello classico[114]. Entrambi vengono tutelati in quanto permettono al singolo di manifestare la propria personalità: la differenza è data dal fatto che mentre il primo si caratterizza per una sua fisicità, il secondo è privo di tale aspetto. Inoltre, se in relazione all'abitazione – e ai singoli luoghi riconosciuti come domicilio – vi sarebbe

[113] La sempre maggiore diffusione dei c.d. *wearable* vale a rendere l'idea della quantità e qualità di dati personali che vengono registrati quotidianamente su di un dispositivo elettronico. Tali apparecchi, indossati direttamente dall'utente o inseriti nei vestiti dello stesso, sono in grado di monitorare, anche 24 ore su 24, il battito cardiaco e le distanze percorse dai loro utilizzatori. Inoltre, a tali dispositivi sono affiancate applicazioni pensate per registrare ciò che viene ingerito quotidianamente in modo da poter controllare la propria dieta.

[114] Cfr. le considerazioni di P. GALDIERI, *Problemi giuridici dell'informatica nel MEC*, Giuffrè, Milano, 1996, p. 214.

una sorta di presunzione riguardante la tipologia delle attività compiute nello stesso, nel sistema informatico tale idea viene meno. Infatti questi si caratterizza per la sua duttilità: esso può essere utilizzato per una molteplicità di scopi, immagazzinando, di conseguenza, dati informatici il cui grado di riservatezza può variare enormemente. In aggiunta, non bisogna dimenticarsi come i dati informatici siano destinati a viaggiare attraverso un gran numero di sistemi informatici diversi. Una tutela ancorata alla fisicità del dispositivo, rischia di essere sproporzionata in eccesso e in difetto[115]. In quest'ottica, il domicilio informatico non si identifica con il sistema informatico, ma ha confini ben più sfumati. Il domicilio informatico sarebbe un luogo immateriale costituito dalle informazioni di carattere personale che si possono trovare all'interno di un determinato elaboratore[116]. Per cui, lo *ius excludendi* cui può fare appello il singolo avrebbe ad oggetto non l'elaboratore ma solo quella porzione del sistema informatico che contiene quei dati personali che vanno a costituire il domicilio informatico.

Più recentemente, non sono mancati Autori che hanno voluto sottolineare maggiormente la problematicità del concetto di domicilio informatico alla luce della capillare diffusione di *smartphone* e di altri dispositivi elettronici. La riflessione muove dall'idea per cui l'analogia tra il domicilio fisico e quello informatico rischierebbe di essere fuorviante a causa della differente qualità di informazioni che possono essere ottenute attraverso la perquisizione di certi *device* elettronici[117]. Infatti, prendendo le mosse da alcune osservazioni fatte

[115] In eccesso, in quanto qualsiasi operazione di accesso ad un sistema informatico, anche quella tendente a ottenere documenti informatici che non contengono informazioni riservate, dovrebbe essere sottoposta al regime autorizzatorio di cui all'art. 14 Cost. In difetto, perché allorché i dati siano transitati, per qualsiasi motivo, in un sistema informatico non di proprietà del soggetto interessato, sembrerebbe venir meno qualsiasi garanzia.

[116] P. GALDIERI, *op. cit.*, p. 218.

[117] Ci si riferisce alle opinioni espresse da A. LEOPIZZI, *La biblioteca (digitale) di Babele. Condotte umane nel cyberspazio e competenza territoriale per le violazioni del domicilio informatico*, in *Giust. pen.*, 2015, III, c. 420.

dalla giurisprudenza nordamericana, viene rilevato come la lettura del contenuto di uno *smartphone* potrebbe costituire una lesione ben maggiore della riservatezza di una persona rispetto ad una tradizionale perquisizione locale o personale. Anche solo tramite l'osservazione delle applicazioni utilizzate dall'utente, sarebbe possibile ipotizzare le sue idee politiche o i suoi orientamenti sessuali. Non solo, l'utilizzazione di strumenti per il *fitness* comporta la memorizzazione sul dispositivo di informazioni sullo stato di salute della persona. In altri termini, il domicilio informatico dovrebbe essere protetto in maniera nettamente diversa e più stringente rispetto a quello classico in ragione della particolarità delle informazioni contenute nel primo.

5. Le garanzie di libertà e segretezza delle comunicazioni

Dopo aver sancito l'inviolabilità della libertà personale e del domicilio, il Costituente ha preso posizione su un altro tema estremamente delicato quale è quello delle garanzie afferenti alla corrispondenza e, più in generale, alle comunicazioni tra singolo individui. Sul punto, la scelta è stata quella di sancirne la libertà e la segretezza[118]. Il rapporto tra questi due elementi è peculiare. In quanto, se da un lato, questi risultano strettamente collegati poiché, la segretezza è funzionale a garantire la libertà di una comunicazione e viceversa; dall'altro lato, entrambi i profili godono di una certa autonomia, essendo possibile immaginare casi in cui uno solo dei due valori venga violato[119].

Passando ad una analisi più precisa dei concetti di libertà e di segretezza di una comunicazione, si può, in primo luogo, affermare come questa possa dirsi libera allorché si esplichi senza alcuna interferenza da parte di privati o di pubblici poteri. Inoltre, la libertà delle comunicazioni è connotata da un duplice profilo, positivo e negativo: infatti l'art. 15 Cost. tutela non solo la libertà positiva che si manifesta attraverso la possibilità per chiunque di poter scegliere con chi comunicare, ma anche quella negativa rappresentata dalla possibilità di decidere di non comunicare con nessuno[120].

Dal canto suo, la segretezza può essere definita in riferimento alla volontà da parte dei conversanti di escludere i terzi dalla conoscenza di quanto viene comunicato. Gli strumenti idonei a manifestare tale intenzione sono i più vari: ciò che conta è che dalla scelta

[118] F. CAPRIOLI, *Colloqui riservati e prova penale*, Giappichelli, Torino, 2000, pp. 42 s., in relazione all'ampiezza della posizione giuridica soggettiva tutelata dall'art. 15 Cost., sottolinea come tale protezione si attivi sia allorché le condotte lesive di tale bene provengano dallo Stato sia quando siano state poste in essere da privati cittadini.

[119] Si pensi al caso del fermo di corrispondenza il quale va a ledere la libertà di comunicazione ma non necessariamente la segretezza della stessa; o all'intercettazione di una comunicazione, la quale è in grado certamente di annullare la garanzia della segretezza delle stesse, lasciandone inalterata la libertà.

[120] Cfr. C. MARINELLI, *op. cit.*, p. 66.

delle modalità emerga il desiderio delle parti di voler evitare che altri individui possano ascoltare quanto viene detto[121]. Per cui, non sono necessarie tecniche particolarmente elaborate. Anche il semplice parlare a bassa voce vale a rendere evidente l'*animus* dei conversanti e a ricomprendere tale comportamento sotto la tutela dell'art. 15 Cost.[122].

Si discute tra gli interpreti sul valore da attribuire all'elemento della segretezza nella ricostruzione della fattispecie tutelata dalla disposizione costituzionale in commento. Infatti, secondo alcuni, da un lato si può affermare come la segretezza delle conversazioni contribuisca a garantirne la libertà e, dall'altro, come la mancanza della riservatezza di una comunicazione non vale a far fuoriuscire la stessa dall'àmbito applicativo dell'art. 15 Cost.[123]. Le comunicazioni di cui il mittente non si sia premurato di controllare la segretezza sarebbero comunque protette dalla garanzia della libertà. In contrapposizione a questa posizione, vi è chi sostiene come l'art. 15 Cost. disegni un'unica fattispecie applicativa formata da due elementi, i quali devono sussistere entrambi per l'emersione della tutela costituzionale[124]. Ciò comporta come conseguenza che tutte le comunicazioni non segrete siano da considerarsi escluse dalla tutela apprestata dall'art. 15 Cost. La distinzione non è di poco conto. Infatti le

[121] In tal senso, F. CAPRIOLI, *op. cit.*, p. 45.

[122] La dottrina, non solo costituzionalistica, ha discusso sull'estensione della segretezza della comunicazione. In particolare, è stato oggetto di dibattito il tema della riconducibilità all'interno dell'art. 15 Cost. del diritto del mittente ad evitare che il destinatario possa divulgare quanto appreso tramite la comunicazione. Gli orientamenti dottrinali sul punto sono riferibili a tre filoni. Secondo il primo, la segretezza delle comunicazioni impone al destinatario di non divulgare quanto egli è venuto a sapere dal mittente senza il suo consenso. L'interesse protetto dall'art. 15 Cost. sarebbe quello a che certe notizie siano conosciute solo da determinate persone prescelte da chi effettua la comunicazione. Diversamente, vi è chi pur ammettendo che la *ratio* della tutela della Costituzione sia quella di garantire la non divulgazione al pubblico di certe informazioni, ritiene, tuttavia, coperte dalla disposizione costituzionale solo le abusive interferenze nelle comunicazioni e non l'illecita divulgazione delle stesse da parte del destinatario. Infine, altri Autori sottolineano come l'oggetto della garanzia sia solo ed esclusivamente la comunicazione in quanto tale e non il diritto del singolo a non veder divulgate notizie personali. Per una più ampia ricostruzione delle posizioni citate, si rinvia a F. CAPRIOLI, *op. cit.*, pp. 50 ss., il quale fa suo l'ultimo orientamento citato.

[123] Cfr. P. BARILE, *op. cit.*, pp. 164 s.

[124] In tal senso, A. PACE, *Problematica*, cit., pp. 247 s.

comunicazioni non segrete, seppur dirette ad un individuo determinato, verrebbero ricomprese nella tutela apprestata dall'art. 21 Cost. e assoggettate ai limiti connaturati alla natura, a questo punto, pubblica dell'esternazione[125].

Chiarite sommariamente le nozioni di libertà e segretezza delle comunicazioni, diventa opportuno concentrarsi sul concetto stesso di comunicazione. La tutela di cui all'art. 15 Cost. si attiva, infatti, solo allorché sussista una tale situazione di fatto. Dallo studio della dottrina costituzionalistica sul tema, emergono due principali correnti di pensiero: una più restrittiva e una più estensiva. La prima, autorevole ma minoritaria, prende le mosse da una visione di insieme circa i beni che sono tutelati dagli artt. 13, 14 e 15 Cost. In queste disposizioni il costituente ha inteso, prima di tutto, proteggere la libertà in senso fisico, per poi ampliare l'àmbito di tutela anche alle manifestazioni spaziali – il domicilio – o spirituali – la corrispondenza – della stessa[126]. Partendo da tale premessa, vi è chi giunge a ritenere che le previsioni di cui all'art. 15 Cost. andrebbero riferite esclusivamente alle espressioni spirituali comunemente intese, escludendo, quindi, dall'oggetto di tutela tutta la corrispondenza non epistolare[127]. Infatti se la *ratio* sottesa alla disposizione in commento è quella di garantire una certa libertà di espressione, allora solo le forme espressive intese come tali dalla generalità dei consociati debbono costituire oggetto di tutela[128].

La dottrina maggioritaria, seguita dalla giurisprudenza costituzionale, accetta una nozione più ampia di comunicazione. Secondo questo indirizzo, la tutela dell'art. 15 Cost. si

[125] Sul punto, A. PACE, *Problematica*, cit., pp. 244 s.

[126] Così si esprime A. PACE, sub *art. 15*, in *Commentario della Costituzione. Rapporti civili*, a cura di G. Branca, Zanichelli, Bologna, 1977, p. 82.

[127] Ancora, A. PACE, sub *art. 15*, cit., pp. 82 s.

[128] L'Autore si preoccupa di evitare un'eccessiva dilatazione della fattispecie tutelata dalla Costituzione; A. PACE, *Problematica*, cit., p. 242 rileva come se si ammettesse che qualsiasi atto comunicativo fosse tutelato dall'art. 15 Cost. si potrebbe andare incontro all'incostituzionalità di numerose disposizioni che, vietando determinati comportamenti, limiterebbero la libertà di comunicazione.

estende a qualsiasi forma di comunicazione indipendentemente dal mezzo che viene utilizzato dai soggetti comunicanti[129]. Infatti nel concetto di libertà di comunicare è ricompreso anche il diritto a scegliere la forma più idonea per manifestare il proprio pensiero, senza che la preferenza per un certo metodo faccia venir meno la tutela costituzionale. In altri termini, se è pur vero che ogni mezzo di comunicazione porta con sé un certo livello variabile di sicurezza, ai fini dell'inquadramento del mezzo all'interno della fattispecie di cui all'art. 15 Cost. è necessario esclusivamente che lo strumento utilizzato sia riconosciuto da chi comunica come idoneo a recapitare un messaggio[130]. Più precisamente, gli elementi che devono sussistere in una comunicazione affinché questa sia protetta dalla Costituzione sono due. In primo luogo, la comunicazione deve avvenire tra almeno due persone determinate o determinabili[131]. Questo requisito vale a differenziare la tutela apprestata dall'art. 15 Cost., rispetto a quella dell'art. 21 Cost., il quale si fa garante della libertà di manifestazione del pensiero[132]. In secondo luogo, la comunicazione deve essere attuale: con ciò si fa riferimento al fatto che la garanzia della segretezza, pur estendendosi per un lasso temporale successivo alla ricezione e lettura del messaggio, non è perpetua ma perdura in tanto in quanto o tutti i soggetti la intendano mantenere oppure fino a quando la comunicazione non assume un valore di carattere storico od artistico[133]. L'accettazione di una tale impostazione comporta la sottoposizione sotto l'ombrello dell'art. 15 Cost. di tutte le comunicazioni effettuate tra presenti, di

[129] Cfr. G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Giuffrè, Milano, 1983, p. 6.

[130] Sostanzialmente in tal senso si esprime, tra gli altri, C. TROISIO, *Corrispondenza (libertà e segretezza della)*, in *Enc. giur. Treccani*, Roma, 1988, p. 4.

[131] V. A. VELE, *Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma*, Cedam, Padova, 2011, p. 9.

[132] Sui rapporti tra art. 15 e 21 Cost. la dottrina costituzionalistica riconosce come questi disciplinino in realtà due fattispecie diverse. Il primo non sarebbe una sottospecie del secondo, pur accomunati da un punto di vista "naturalistico" le due disposizioni svolgono funzioni differenti. V. sul punto, P. BARILE, *op. cit.*, p. 165; A. PACE, *Problematica*, cit., p. 243.

[133] Cfr. P. BARILE – E. CHELI, *Corrispondenza (libertà di)*, in *Enc. dir.*, Giuffrè, Milano, 1962, vol. X, p. 745.

quelle compiute tramite segni simbolici, indipendentemente dalla riconoscibilità degli stessi e, infine, di quelle realizzate con mezzi di comunicazione anche diversi da quelli tradizionali.

Sempre in tema di definizione dell'oggetto di tutela dell'art. 15 Cost., deve essere rilevato come questo sia stato ampliato dalla Corte costituzionale oltre quanto precisato in precedenza. Infatti i giudici costituzionali hanno ricompreso all'interno dell'area di operatività della norma costituzionale anche i cosiddetti tabulati telefonici. Il punto di partenza del ragionamento compiuto dal Giudice delle leggi, nella sentenza 11 marzo 1993, n. 81, è rappresentato dall'ampiezza della garanzia apprestata dall'art. 15 Cost. alla libertà e alla segretezza delle comunicazioni, la quale, quindi, è tale da ricomprendere sia la comunicazione in quanto tale sia i dati esteriori della stessa che possono permettere di identificarne i soggetti, la durata e il luogo in cui sia stata effettuata[134]. A sua volta, questa interpretazione estensiva della disposizione costituzionale si giustifica in ragione della stretta connessione tra libertà e segretezza delle comunicazioni e i diritti riguardanti la personalità dell'individuo. Infatti, l'art. 15 Cost., proteggendo un valore espressivo della personalità umana e della vita di relazione, costituisce uno dei diritti fondamentali rientrante tra i supremi valori costituzionali.

Per quanto riguarda il versante soggettivo della tutela apprestata dall'art. 15 Cost., si riconosce comunemente un'estensione del diritto alla libertà e alla segretezza delle comunicazioni a tutti gli individui, indipendentemente dal loro rapporto con l'ordinamento italiano[135]. Per questo motivo, sono titolari del diritto contenuto nella disposizione in discorso sia gli stranieri sia gli apolidi[136].

[134] La sentenza è pubblicata su *Giur. cost.*, 1993, pp. 731 ss.

[135] In tal senso, v. A. VELE, *op. cit.*, p. 9, il quale estende l'àmbito soggettivo della garanzia apprestata dall'art. 15 Cost. anche alle formazioni sociali di cui le singole persone sono membri.

[136] Cfr., *ex multis*, C. MARINELLI, *op. cit.*, p. 68.

Definito l'àmbito applicativo, occorre aggiungere come il Costituente abbia, inoltre, ammesso la possibilità di limitare la libertà e la segretezza delle comunicazioni, purché queste restrizioni siano previste dalla legge e siano disposte dall'autorità giudiziaria. Per quanto riguarda l'ampiezza dello spazio di manovra lasciato al legislatore in tema di misure che possono comprimere il diritto di cui all'art. 15 Cost., una parte della dottrina ha sottolineato la sussistenza di un limite implicito. Infatti, pur potendo considerarsi legittime le disposizioni di legge ordinaria che permettono all'autorità giudiziaria di violare la segretezza delle comunicazioni, sarebbe inibita al legislatore la possibilità di prevedere «blocchi» postali o telefonici[137].

La legittimità di eventuali limitazioni alla libertà e alla segretezza delle comunicazioni non deriva solo dal rispetto dei requisiti formali previsti dal legislatore costituzionale. Infatti in ragione della stretta connessione sussistente tra i diritti inviolabili dell'uomo tutelati dall'art. 2 Cost. e il diritto oggetto dell'art. 15 Cost., si ritiene che quest'ultimo possa essere limitato solo per favorire la tutela di altri beni di preminente rilevanza costituzionale[138]. Sul punto, la Corte costituzionale ha più volte affermato come l'art. 15 Cost. effettui un bilanciamento tra due esigenze contrapposte: da un lato quella della garanzia di un diritto ritenuto connaturato ai diritti della personalità, definiti inviolabili dall'art. 2 Cost., e dall'altro, quella

[137] V., in particolare, P. BARILE, *op. cit.*, p. 165. Nel vigente codice di procedura penale risulta essere presente solo il sequestro della corrispondenza all'art. 254 c.p.p. Il legislatore, conscio della delicatezza dell'atto, ha deciso di circondarlo di particolari cautele. Queste sono da ricercarsi, in primo luogo, nell'esclusione della polizia giudiziaria dal novero dei soggetti che possono disporre il sequestro – nel caso di urgenza è previsto un meccanismo di convalida da parte del pubblico ministero. In secondo luogo, si prevede che l'autorità procedente possa delegare la polizia giudiziaria a effettuare il sequestro del plico o della missiva, il quale, però, deve essere recapitato ancora sigillato al pubblico ministero.

[138] Cfr. G. ILLUMINATI, *op. cit.*, p. 8.

della salvaguardia del potere statutale di poter efficacemente prevenire e reprimere i reati, valore, anch'esso, di sicuro rilievo costituzionale[139].

Ciò posto, la Costituzione impone un livello minimo di garanzie che devono essere rispettate dal legislatore ordinario nella creazione della fattispecie che autorizzi una lesione della segretezza e della libertà delle comunicazioni. La prima di queste è data proprio dalla riserva assoluta di legge, per cui le compressioni dei beni in discorso risultano legittime soltanto nell'ipotesi in cui siano espressamente previste dalla legge e dagli atti aventi forza di legge. Con tale previsione si rende esplicita la volontà di evitare che atti normativi del Governo possano andare ad incidere sui diritti fondamentali dei singoli. Inoltre, sempre nell'ottica di sottrarre al potere esecutivo qualsiasi possibilità di intervento su una materia così delicata, dopo la riserva di legge viene imposta anche una riserva di giurisdizione. Questa si ramifica in una duplice direzione. In primo luogo, è individuato come soggetto che può legittimamente autorizzare una compressione dell'art. 15 Cost. l'autorità giudiziaria. Espressione che nel lessico della Costituzione ricomprende pacificamente tutta la magistratura, quindi sia il pubblico ministero sia il giudice procedente[140]. In secondo luogo, si impone che l'autorizzazione alla compressione dei diritti in discorso sia concessa attraverso un atto motivato della stessa. L'obbligo di motivazione previsto a carico del magistrato procedente ha, in tutta

[139] Così Corte cost., 6 aprile 1973, n. 34, cit. In senso conforme alla pronuncia citata, v. Corte cost., 26 febbraio 1993, n. 81, cit.; Corte cost. 23 luglio 1991, n. 366, in *Giur. cost.*, 1991, pp. 2914 ss.

[140] Il significato minimo da attribuire a tale espressione è sicuramente quello di evitare che il potere esecutivo possa andare ad interferire con la libertà e segretezza delle comunicazioni. Dal canto suo, la pubblica amministrazione, come riconosciuto da Corte cost., 16 luglio 1968, n. 100 in *Giur. cost.*, 1968, pp. 1587 ss., ha esclusivamente il potere di sollecitare l'intervento dell'autorità giudiziaria. Sull'estensione del termine «autorità giudiziaria» una parte minoritaria della dottrina ritiene che questa espressione faccia riferimento esclusivamente al giudice. Il ragionamento procede per analogia: l'autorità giudiziaria di cui all'art. 13 Cost. che può legittimamente limitare la libertà personale è solo quella giurisdizionale, in quanto, a norma dell'art. 111, co. 7° Cost. i provvedimenti sulla libertà personale sono pronunciati da organi giurisdizionali. Individuato così il significato dell'espressione «autorità giudiziaria», non può che ritenersi lo stesso uguale in tutta la Costituzione. La conseguenza di un tale ragionamento sarebbe il divieto di disporre alcuna limitazione delle comunicazioni da parte del pubblico ministero. Cfr. L. FILIPPI, *L'intercettazione di comunicazioni*, Giuffrè, Milano, 1997, p. 60.

evidenza, l'obiettivo di poter permettere il controllo sulla legittimità della scelta compiuta ed, eventualmente, di poter sottoporre ad impugnazione il provvedimento impugnato[141].

A differenza degli artt. 13, 14 Cost., i quali, come è noto, hanno per oggetto la libertà personale e l'inviolabilità del domicilio, l'art. 15 Cost. non prevede che la libertà e la segretezza delle conversazioni possano essere limitate in via d'urgenza.

La lacuna è, secondo la dottrina maggioritaria, intenzionale e non frutto di una svista del Costituente[142]. La ragione di una tale scelta sarebbe duplice. La prima sarebbe da ricercare nelle differenze strutturali che accompagnano le limitazioni della libertà personale o di quella domiciliare rispetto a quelle in tema di segretezza e libertà delle comunicazioni. Infatti, mentre nel primo caso è, almeno in via tendenziale, solo il soggetto sottoposto ad indagine a subire una compressione di un proprio diritto fondamentale; allorché, invece, si faccia riferimento ad un atto di intercettazione, le sfere colpite da un tale provvedimento sono almeno due: quella del soggetto indagato e quella del soggetto che, pur conversando con il primo, può essere del tutto estraneo al procedimento penale[143]. La seconda argomentazione è di tipo sia strutturale sia storico. Infatti sicuramente i Costituenti quando affrontarono la questione circa la possibilità di consegnare un potere, seppur temporaneo, all'autorità di pubblica sicurezza in tema di limitazione della libertà e segretezza delle comunicazioni avevano in mente gli abusi perpetrati durante il regime fascista e non solo[144]. Inoltre, la natura stessa degli atti che possono andare ad incidere sulla riservatezza delle comunicazioni sembrava consigliare una certa cautela riguardo alla possibilità di ammettere un potere da parte

[141] Così, C. MARINELLI, *op. cit.*, p. 70.

[142] In senso opposto, v. P. BARILE – E. CHELI, *Corrispondenza*, cit., p. 749.

[143] V., tra i tanti, P. BARILE, *op. cit.*, p. 169. Più recentemente, A. VELE, *op. cit.*, p. 13.

[144] Sul punto, per una ricostruzione storica, si rimanda a U. GUSPINI, *L'orecchio del regime: le intercettazioni telefoniche al tempo del fascismo*, Milano, Mursia, 1973, *passim*.

della polizia. Come chiarito dalla dottrina, trattandosi di atti che vengono compiuti in assenza dell'interessato e a sua insaputa, questi costituiscono una tipologia di provvedimenti nei quali è più frequente che si verifichino arbitrii[145]. Infatti se anche solo la mera presenza dell'indagato può essere considerato un limite quantomeno psicologico all'abuso del funzionario di pubblica sicurezza, questa barriera viene meno tanto nel fermo della corrispondenza quanto nelle intercettazioni di comunicazioni[146].

Ulteriori elementi di precisazione circa il contenuto della tutela apprestata dall'art. 15 Cost. alla libertà e segretezza delle comunicazioni vengono dall'analisi della giurisprudenza costituzionale in tema di intercettazioni di conversazioni telefoniche. Questa, pur avendo come oggetto un ben specifico mezzo di ricerca della prova, può tuttavia, essere utile all'interprete per chiarire meglio i requisiti richiesti ai fini della legittimità delle limitazioni della libertà e della segretezza delle conversazioni. L'obiettivo principale cui tendono i giudici costituzionali è quello di andare alla ricerca di un bilanciamento tra le esigenze di tutela del diritto del singolo indagato che si trovi a subire l'atto di intercettazione e i prominenti interessi pubblicistici sottesi alla repressione dei reati. Nel far ciò la Corte costituzionale si preoccupa di precisare quali debbano essere i limiti e le garanzie entro i quali è ammessa l'attività di intercettazione da parte dell'autorità. Questi sono ben precisati in una ormai storica sentenza degli anni '70, nella quale si chiarisce come una normativa in tema di intercettazioni che sia rispettosa del dettato dell'art. 15 Cost. dovrebbe, in primo luogo, permettere l'inter-

[145] V. P. BARILE, *op. cit.*, p. 168; A. PACE, *Problematiche*, cit., p. 264.

[146] Cfr. A. PACE, *Problematiche*, cit., p. 264.

cettazione di conversazioni telefoniche soltanto allorché sussistano effettive esigenze connesse allo svolgimento delle indagini per un determinato reato[147]. In secondo luogo, dovrebbero essere previste da un lato, le modalità che rendano l'atto di intercettazione limitato nel tempo e dall'altro, strumenti tecnici idonei a garantire che venga intercettato solo il soggetto nei confronti del quale si vuole investigare. Un ruolo fondamentale in questa prospettiva, spetterebbe al giudice. Infatti il magistrato non solo sarebbe tenuto a dare conto della sussistenza dei presupposti elencati all'interno del provvedimento autorizzativo, ma, inoltre, nel momento dell'effettiva predisposizione di una limitazione alla segretezza e alla libertà delle comunicazioni, avrebbe il compito di calibrare correttamente, in relazione alla fattispecie concreta, il potere di intercettazione.

La tutela del rispetto della corrispondenza non è esclusivamente affidata alla nostra Costituzione, in quanto anche la C.e.d.u. prende posizione sul tema all'art. 8, § 1 C.e.d.u. Sul punto, la prima distinzione che deve essere effettuata è quella, in linea con quanto affermato prima in relazione alla Carta costituzionale, tra la libertà di espressione e quella di corrispondenza. Mentre con la prima l'oggetto della garanzia è dato da ciò che una persona afferma, con la seconda si concentra l'attenzione sul mezzo utilizzato per esprimere il proprio pensiero[148]. Posta tale distinzione, l'utilizzo del termine corrispondenza non deve trarre in inganno. Infatti oggetto della tutela non sono solo le comunicazioni effettuate tramite il servizio postale, ma, più in generale, tutte le comunicazioni tra due o più persone. Ciò che viene garantito è il diritto di ciascun individuo di far sì che ciò che viene detto o scritto in una conversazione privata, ossia sottratta con le normali cautele al pubblico, rimanga tale. Lungo questo crinale, la definizione di corrispondenza è stata facilmente estesa da parte dei giudici

[147] Ci si riferisce a Corte cost., 6 aprile 1973, cit.

[148] In relazione alla C.e.d.u., v. M. MURGO, *Il diritto*, cit., p. 1183.

di Strasburgo alla materia delle intercettazioni telefoniche, alle registrazioni di conversazioni avvenute nel domicilio, alle e-mail e alla sorveglianza mediante G.P.S.[149]. Quello che viene tutelato attraverso l'art. 8, § 1 C.e.d.u. sono il mezzo di comunicazione e l'aspettativa del singolo circa il livello di segretezza della conversazione in relazione allo strumento utilizzato. In questo filone si inserisce la tutela apprestata dalla Corte all'acquisizione dei tabulati telefonici. Questa è, ovviamente, riconosciuta come qualcosa di diverso rispetto ad un'intercettazione, in quanto non permette di conoscere il contenuto della conversazione. Tuttavia, il numero di telefono chiamato da una persona, la durata delle telefonate e tutti i dati esterni alla comunicazione sono intesi dalla Corte come parte integrante della comunicazione stessa e sono, quindi, ricompresi nel concetto di corrispondenza di cui all'art. 8, § 1 C.e.d.u.[150]. Ponendosi sulla stessa linea, la Corte ha avuto modo di sottolineare come la probabile violazione dell'art. 8, § 1 C.e.d.u. sia indipendente da un eventuale utilizzo del materiale raccolto da parte dell'autorità procedente[151].

L'art. 8 C.e.d.u. non si limita solamente a sancire il diritto al rispetto delle comunicazioni, ma, secondo un modello comune alle carte dei diritti, nel § 2 elenca quelle che sono le modalità attraverso le quali il diritto tutelato dal § 1 può venire legittimamente compresso per soddisfare altre esigenze. Tali modalità sono precisamente individuate dalla Convenzione e svolgono la funzione di limitare il potere statale di ingerenza nella vita dei singoli

[149] Cfr. Corte eur., 6 settembre 1978, Klass e altri c. Germania, § 41; Corte eur., 1° giugno 2004, Narinen c. Finlandia, § 32; Corte eur. 3 aprile 2007, Copland c. Regno Unito, § 44; Corte eur., 25 giugno 1997, Halford c. Regno Unito, § 44.

[150] In tal senso, Corte eur., 2 agosto 1984, Malone c. Regno Unito, § 84.

[151] Cfr. Corte eur., 25 marzo 1998, Kopp c. Svizzera, §§ 52, 53.

individui. Il primo limite cui deve farsi riferimento è quello della espressa previsione dell'interferenza all'interno di una disposizione di carattere legislativo, sintetizzato nell'espressione «*in accordance with the law*».

Il termine «*law*», ovviamente, pone non pochi problemi di definizione in relazione soprattutto alle differenti tradizioni giuridiche dei Paesi membri del Consiglio d'Europa. Tuttavia, la Corte, come sempre in questi casi, si preoccupa di individuare una nozione di legge autonoma e indipendente rispetto a quella accettata dai singoli ordinamenti degli Stati. Per fare questo, i giudici di Strasburgo pongono al centro della loro riflessione la *ratio* sottesa al principio di legalità. Questa è individuata nell'esigenza di evitare che gli individui possano subire una limitazione ai loro diritti fondamentali, sulla base di atti arbitrari dell'autorità pubblica. Tenendo conto dell'obiettivo perseguito, ossia quello di arginare la discrezionalità degli Stati, la Corte riscostruisce il concetto di legge in maniera relativamente elastica. In primo luogo, viene esclusa l'idea che il richiamo dell'art. 8, § 2 C.e.d.u. alla legge, contenuto anche in altre disposizioni, debba essere inteso alla sola legge in senso formale[152]. In questa prospettiva, un'utile base giuridica per legittimare un'interferenza in un diritto fondamentale può anche essere trovata in una disposizione non scritta[153]. Quello che, però, deve essere garantito in ogni caso è la certezza del diritto.

Per questo la Corte prosegue nella sua analisi del principio di legalità per andare ad enucleare i due elementi che rendono un provvedimento dell'autorità pubblica rispettoso del canone della legalità. Questi sono l'accessibilità e la prevedibilità[154]. Con la prima, si fa riferimento al fatto che la base giuridica dell'atto sia stata adeguatamente pubblicizzata, il che

[152] Così la Corte e.d.u. si esprime nel *leading case* Corte eur., 26 aprile 1979, Sunday Times c. Regno Unito, §§ 47-49.

[153] V., in particolare, Corte eur., 26 aprile 1979, Sunday Times c. Regno Unito, § 47.

[154] Cfr. A. CISTERNA, *op. cit.*, p. 215.

vuol dire che un cittadino deve poter avere le giuste indicazioni circa le norme applicabili in una data situazione. Con la seconda, viene presa in considerazione la qualità dell'atto normativo: questo deve essere chiaro e preciso. A loro volta, questi requisiti sussistono soltanto se la legge è in grado di indirizzare il comportamento del cittadino, il quale deve poter prevedere le conseguenze delle proprie azioni[155]. Ovviamente, prosegue la Corte, un certo livello di indeterminatezza è connaturato a qualsiasi provvedimento normativo, mentre chiarezza e precisione non devono mai andare a discapito della flessibilità e dell'adattabilità della legge alle varie fattispecie concrete[156]. È compito del legislatore nazionale trovare il giusto bilanciamento. Infatti il termine prevedibilità non deve essere inteso in senso eccessivamente restrittivo. Per quanto una disposizione possa essere scritta in maniera corretta, rimane sempre un margine di interpretazione affidato alle autorità giurisdizionali. Tale margine di apprezzamento non è di per sé contrario al concetto di prevedibilità. Si tratta, piuttosto, di controllare l'ampiezza della discrezionalità alla luce del numero e dello *status* delle persone coinvolte, del campo di applicazione della norma e del contenuto dello strumento giuridico[157].

La Corte europea dei diritti dell'uomo prosegue la sua individuazione dei requisiti che possono rendere una limitazione di un diritto fondamentale legittima, ponendo la sua attenzione sui rimedi esperibili. Infatti, altro requisito, implicito alla formula «*in accordance with the law*», è quello di garantire la possibilità di un controllo sull'atto che ha compresso un diritto fondamentale. Sarebbe contrario ai princìpi dello Stato di diritto, attribuire all'auto-

[155] Cfr., ancora, Corte eur., 26 aprile 1979, Sunday Times c. Regno Unito, § 49.

[156] V. Corte eur., 24 marzo 1988, Olsson c. Svezia, § 61.

[157] Cfr. Corte eur. Grande Chambre, 10 novembre 2005, Leyla Şahin c. Turchia, § 91.

rità pubblica un potere che possa incidere sui diritti fondamentali dell'individuo senza prevedere alcuna forma di verifica circa la correttezza dell'esercizio di tale potere. Ovviamente, una tale impostazione ha rilevanti conseguenze per quanto attiene alle modalità di formulazione della disposizione attributiva del potere. Questa deve chiarire in maniera espressa lo scopo che si intende perseguire e le modalità con cui si vuole raggiungere l'obiettivo[158].

Oltre ad essere prevista dalla legge, la limitazione dei diritti protetti all'art. 8, § 1 C.e.d.u. deve giustificarsi alla luce delle finalità elencate dall'art. 8, § 2 C.e.d.u., le quali costituiscono un insieme tassativo di cause che possono giustificare la compressione di un diritto fondamentale da parte dello Stato. Queste possono, a loro volta, essere ricondotte a tre macro-aree: la prima è quella afferente agli interessi di sicurezza di ciascuno Stato, ossia alla tutela dell'ordine pubblico, della sicurezza e della difesa nazionale, dell'imparzialità e dell'autorità del potere giudiziario; la seconda, fa riferimento a quegli elementi ricompresi nel concetto di tutela del corpo sociale, alludendo, in questo senso al benessere economico di uno Stato, alla lotta alla criminalità, alla protezione della salute pubblica; l'ultima categoria ricomprende gli interessi dei privati, i quali sono quelli corrispondenti al diritto di libertà e di reputazione. Questi requisiti, inoltre, devono essere letti attraverso la lente della necessità di garantire che l'ingerenza si giustifichi in relazione al mantenimento di una società democratica[159].

Questi elementi vengono calati dalla Corte nella complessa tematica delle intercettazioni, predisponendo i necessari adattamenti in relazione alla complessità e particolarità dello strumento.

---

[158] In tal senso, v. Corte eur. Grand Chambre, 17 febbraio 2004, Maestri c. Italia, § 30.

[159] Su tale concetto, si richiamano le considerazioni di A. CISTERNA, *op. cit.*, pp. 221 ss.; A. GALLUCCIO, *Profili generali sugli art. 8-11*, in *Corte di Strasburgo e giustizia penale*, a cura di G. Ubertis – F. Viganò, Giappichelli, Torino, 2016, pp. 258 s.

In proposito, l'attenzione della Corte si è per lo più concentrata sul lato del controllo di legittimità di tali atti alla luce delle garanzie previste dalla Convenzione.

Sul punto, i giudici di Strasburgo ammettono l'esistenza di un certo margine di discrezionalità nelle scelte del legislatore nazionale[160]. Infatti, spetta a questo trovare, in prima battuta, il giusto bilanciamento tra le esigenze di repressione e controllo dei fenomeni criminali e quelle di tutela dei diritti dei singoli. I profili sui quali la Corte si sofferma riguardano rispettivamente, la natura, lo scopo e la durata delle misure, i presupposti per l'autorizzazione a porre in essere tali misure, l'autorità che controlla lo svolgimento delle operazioni e, infine, la tipologia dei rimedi offerta dall'ordinamento nazionale per evitare abusi[161].

Per quanto concerne il rispetto del principio di legalità delicato è il problema relativo alla prevedibilità della misura. Infatti sicuramente imporre un qualche tipo di obbligo di avviso da parte della polizia verso le persone oggetto di intercettazione priverebbe lo strumento della sua efficacia, rendendolo sostanzialmente inutile. La Convenzione non richiede, in sostanza, che la legge nazionale possa permettere ad un individuo di prevedere quando sarà sottoposto ad intercettazione e, quindi, di mutare di conseguenza il suo comportamento[162]. Tuttavia, questa considerazione non autorizza a ritenere inapplicabile il requisito della prevedibilità alla fattispecie delle intercettazioni. Ciò in quanto proprio la materia in discorso rappresenta una delle più delicate per quanto riguarda il timore di atti arbitrari da parte dell'autorità pubblica. Per questo motivo, la Corte precisa come il compito del legislatore sia quello di individuare con precisione i casi e i modi attraverso cui possa essere violato il se-

[160] V. Corte eur., 6 settembre 1978, Klass e altri c. Germania, § 48.

[161] Ancora, Corte eur., 6 settembre 1978, Klass e altri c. Germania, § 50.

[162] Cfr. Corte eur., 26 marzo 1987, Leander c. Svezia, § 51.

greto delle conversazioni, dando, così, a ciascun cittadino la possibilità di sapere a quali condizioni e con quali modalità potrebbe, teoricamente, venir leso il suo diritto al segreto nelle conversazioni[163].

Parzialmente diverso è il discorso in tema di controlli della legittimità dell'azione della pubblica autorità e del diritto del singolo ad essere informato delle operazioni compiute. Su quest'ultimo aspetto, la Corte, almeno per quanto riguarda le operazioni di sorveglianza compiute dall'*intelligence*, non impone agli Stati contraenti l'obbligo di avvisare la persona intercettata al termine dell'atto[164]. Questo perché un meccanismo così rigido potrebbe rendere infruttuose operazioni di sorveglianza sul lungo periodo. Tuttavia, a fare da contrappeso ad una tale impostazione, vi è la tematica dei controlli. La Corte, infatti, riconosce che proprio quei mezzi di controllo attuati all'insaputa del cittadino siano quelli più delicati, nei quali maggiore è il rischio di un utilizzo arbitrario. Proprio per questo motivo i giudici di Strasburgo sottolineano come, almeno al termine di tutta la procedura, debba essere prevista una qualche forma di controllo da parte del potere giudiziario, il quale costituisce il miglior garante del rispetto della legalità[165]. Onde consentire, poi la possibilità di una verifica *ex post*, le norme che attribuiscono il potere di disporre un'intercettazione devono precisare gli illeciti per i quali queste possono essere disposte, i termini temporali delle operazioni, le procedure attraverso le quali i dati ottenuti sono conservati e utilizzati[166].

[163] In tal senso, Corte eur., 2 agosto 1984, Malone c. Regno Unito, § 67; Corte eur., 25 marzo 1998, Kopp c. Svizzera, § 64.

[164] La Corte e.d.u. stessa ha precisato come la disciplina delle operazioni di sorveglianza non possa differire eccessivamente da quella prevista per le intercettazioni, v., ad esempio, Corte eur., 1° luglio 2008, Liberty e altri c. Regno Unito, § 63.

[165] Così, Corte eur., 6 settembre 1979, Klass e altri c. Germania, § 55.

[166] In tal senso, Corte eur., 29 giugno 2006, Weber e Saravia c. Germania § 95; Corte eur., 24 aprile 1990, Huvig c. Francia, § 34.

Per quanto riguarda i reati tali da giustificare l'adozione di una tale misura, la Corte riconosce come il requisito della prevedibilità non imponga necessariamente la creazione di una lista dettagliata degli illeciti per i quali possa essere disposta un'intercettazione, potendo ritenersi rispettosa della Convenzione anche una normativa che faccia genericamente riferimento a casi di sicurezza nazionale[167].

Volgendo l'attenzione alla normativa italiana sul tema, la dottrina, analizzando la disciplina contenuta negli artt. 266 ss. c.p.p., non ha mancato di criticare alcune delle scelte compiute dal legislatore, evidenziando, principalmente, come più volte gli interessi connessi all'accertamento e alla repressione dei reati siano stati giudicati preminenti rispetto al diritto del singolo di veder salvaguardata la propria libertà e segretezza delle comunicazioni. Una prima critica è stata formulata nei confronti del catalogo di reati per i quali è ammessa l'intercettazione: in essa sarebbero presenti alcune fattispecie di scarsa gravità – come le molestie telefoniche – per le quali sembrerebbe eccessivo ammettere il potere di disporre delle intercettazioni[168].

Altro filone di critiche, riguarda l'impossibilità per il giudice che autorizza la captazione della possibilità di calibrare la compressione del diritto di cui all'art. 15 Cost. in relazione al reato per cui si procede, graduando, anche in relazione alla situazione concreta, il livello di intrusione nella vita privata dei singoli[169].

---

[167] Cfr. Corte eur., 18 maggio 2010, Kennedy c. Regno Unito, §§ 159, 160.

[168] V P. BALDUCCI, *op. cit.*, p. 41, L. FILIPPI, *op. cit.*, p. 49; C. MARINELLI, *op. cit.*, p. 71.

[169] Secondo P. BALDUCCI, *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria*, Giuffrè, Milano, 2002, p. 42 si potrebbe ipotizzare un sistema in cui il giudice sulla base della gravità non solo del reato, ma anche del fatto concreto possa decidere quale limitazione della segretezza e libertà delle conversazioni sia più opportuna nel caso concreto. La scala dei provvedimenti adottabili andrebbe dalla semplice acquisizione dei dati esteriori delle comunicazioni fino alla possibilità di svolgere intercettazioni direttamente nel domicilio in caso di particolari esigenze. In un'ottica *de lege ferenda* una tale opzione interpretativa potrebbe essere un buono spunto di partenza per il legislatore per regolare la materia della raccolta di elementi probatori attraverso gli strumenti elettronici: il grado minimo sarebbe rappresentato dalla richiesta ai fornitori di connettività dei dati relativi alla

Inoltre, è stata sottoposta a critica sia la mancanza di un limite massimo di durata per le intercettazioni – le quali possono durare per tutta la fase delle indagini – sia la mancanza di uno strumento adeguato di impugnazione[170].

navigazione di un soggetto, l'ipotesi più invasiva sarebbe, invece, quella dell'utilizzo del c.d. captatore informatico.

[170] Cfr. C. MARINELLI, *op. cit.*, p. 73.

Capitolo IV

Le prove informatiche di carattere "tipico"

SOMMARIO: 1. Le ispezioni e le perquisizioni informatiche – 2. Il sequestro di materiale informatico – 3. L'acquisizione di dati di carattere informatico – 4. La conservazione dei dati relativi al traffico telematico per finalità afferenti alle indagini penali – 5. Le intercettazioni di comunicazioni informatiche o telematiche

1. Le ispezioni e le perquisizioni informatiche

Il codice di procedura penale originariamente non conteneva alcuna disposizione riguardante la tematica della *digital evidence*. Evenienza agevolmente comprensibile sulla base del periodo storico in cui lo stesso è stato emanato. Il primo intervento volto a permettere l'ingresso nel processo penale delle tecnologie informatiche è dei primi anni '90, quando, tramite la l. 23 dicembre 1993, n. 547, è stato introdotto l'art. 266 *bis* c.p.p.[1]. Dopo questo primo provvedimento, è seguito un periodo di relativo silenzio, in cui, nonostante la ratifica della Convenzione di Budapest sul *cybercrime* del 2001, il legislatore non è intervenuto per regolare gli aspetti problematici delle prove di carattere informatico. Solo tramite la l. 18 marzo 2008, n. 48, si è, finalmente, dato ingresso nell'ordinamento italiano ai princìpi della *computer forensics* presenti nella convenzione citata. La caratteristica principale dell'intervento legislativo è data sicuramente dalla sua disorganicità. Infatti la l. n. 48/2008, anche a causa del

[1] V., sul punto, Cap. II, § 4.

momento politico in cui è stata approvata, invece di disegnare un sistema autonomo di acquisizione, analisi e valutazione delle evenienze informatiche, si è occupata di interpolare singole disposizioni del codice di rito penale[2]. Proprio la frammentarietà dell'intervento legislativo rende particolarmente difficoltosa lo svolgimento di un discorso unitario sul punto. Per questo motivo, si è preferito procedere attraverso un'analisi che ripercorra singolarmente i diversi istituti toccati dalla modifica legislativa.

Tra questi risultano di primaria importanza le ispezioni e le perquisizioni[3]. Si tratta, come è agevole intuire anche dalla loro collocazione sistematica nel Capo III del Libro III del codice di rito penale, di due mezzi di ricerca della prova. Le prime svolgono la funzione di permette all'autorità procedente di «accertare le tracce e gli altri effetti materiali del reato» oppure, se queste risultano disperse o inesistenti, di descrivere lo stato attuale del luogo o della persona su cui viene svolta l'ispezione. Le seconde, invece, hanno una natura più versatile, in quanto svolgono una duplice funzione: da un lato, permettono l'acquisizione al procedimento penale del corpo del reato o delle cose pertinenti allo stesso; dall'altro, possono essere disposte allorché vi sia il fondato motivo di ritenere che in un determinato luogo possa essere eseguito l'arresto dell'imputato o dell'evaso[4].

Ad una prima, sommaria, lettura la distinzione tra questi due strumenti sarebbe data dall'attività compiuta dall'autorità procedente: descrittiva nel caso dell'ispezione, tesa alla

[2] Come sottolineato da L. LUPÁRIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc.*, 2008, p. 718, la normativa è stata approvata frettolosamente a causa della caduta del Governo e del successivo scioglimento delle Camere.

[3] Oltre ai contributi citati successivamente, per alcune considerazioni di carattere generale su perquisizioni e ispezioni si rimanda a P. BALDUCCI, *Perquisizione (diritto processuale penale)*, in *Enc. dir.*, Giuffrè, Milano, 2000, agg. IV, pp. 979 ss.; M. BARGIS, *Perquisizione*, in *Dig. pen.*, Utet, Torino, 1995, pp. 488 ss.; P. BELLORA, *Ispezione giudiziale*, in *Dig. pen.*, Utet, Torino, 1993, vol. VII, pp. 275 ss.; V. FRONZONI, *Perquisizioni*, in *Enc. giur. Treccani*, 2007, pp. 1 ss.; P. MOSCARINI, *Ispezione (diritto processuale penale)*, in *Enc. dir.*, Giuffrè, Milano, 1998, agg. II, pp. 464 ss.

[4] Il termine «arresto» utilizzato dal legislatore non deve, secondo la dottrina, essere interpretato in senso tecnico, ma, piuttosto comprensivo di tutte quelle ipotesi di ricerca dell'imputato o indagato al fine di operare una restrizione alla sua libertà personale. Cfr. P. FELICIONI, *Le ispezioni e perquisizioni*, Giuffrè, Milano, 2° ed., 2012, p. 96.

ricerca di un *quid* nel caso della perquisizione. Un'autorevole dottrina afferma che chi effettua un'ispezione usa gli occhi, mentre chi compie una perquisizione utilizza le mani[5]. Volendo scendere più nello specifico, discusso è il tema riguardante la distinzione tra i due atti in discorso allorché si utilizzino degli strumenti tecnici. In particolare, oggetto di discussione è stata la sottoposizione a radiografie del soggetto sospettato di trasportare ovuli di sostanze stupefacenti all'interno del proprio corpo. Secondo alcuni tale pratica, finalizzata, inoltre, a garantire la salute del soggetto, può farsi rientrare nel concetto di perquisizione[6]. Infatti in tale evenienza si tratterebbe pur sempre di un'attività finalizzata alla ricerca e al sequestro del corpo del reato. Diversamente, altri sostengono come tale atto sia in ogni caso definibile come ispezione personale, in quanto la perquisizione presuppone una ricerca di carattere "fisico" che difetterebbe in tale situazione[7].

Tuttavia, il vero nodo problematico da sciogliere ai fini del presente lavoro riguarda l'individuazione dei confini delle due fattispecie nel caso di ispezione o perquisizione su sistema informatico. Infatti, come fatto notare dalla dottrina, nel caso in cui l'oggetto della ricerca sia immateriale, la differenza tra i due atti rischia di sfumare. La questione non è solo di carattere meramente dogmatico, in quanto ad essa si ricollegano importanti conseguenze. Tra queste, sicuramente la più importante riguarda l'applicabilità dell'art. 256 c.p.p. in tema di opposizione del segreto giornalistico, disciplinato in relazione al sequestro[8].

Sul tema si registrano almeno due opinioni differenti. Per un primo orientamento, che riecheggia la tradizionale distinzione tra ispezione e perquisizione, deve essere valorizzato

[5] Ci si riferisce a F. CORDERO, *Procedura penale*, Giuffrè, Milano, 9° ed., 2012, p. 827.

[6] Cfr., L. D'AMBROSIO, *La pratica di polizia giudiziaria*, I, *La polizia giudiziaria nel processo penale*, Cedam, Padova, 7° ed., 2007, p. 339.

[7] Cfr., P. FELICIONI, *op. cit.*, pp. 142 s.

[8] V., A. CISTERNA, *Perquisizioni in caso di fondato motivo*, in *Guida dir.*, 2008, f. 16, p. 66.

l'obiettivo che si vuole perseguire attraverso l'atto compiuto. Qualora la finalità sia quella di constatazione e verifica del sistema informatico, effettuata anche mediante clonazione dello stesso, si tratterebbe di ispezione[9]. Viceversa, allorché l'obiettivo sia quello della apprensione e successivo sequestro di dati informatici, saremmo nell'àmbito della perquisizione.

Per un secondo e differente indirizzo, il confine tra i due atti può essere tracciato alla luce del dato normativo. Il punto di partenza delle argomentazioni è costituito dall'art. 247, co. 1° *bis* c.p.p., il quale prevede la possibilità di effettuare un'attività di ricerca su di un *device* elettronico ancorché questo sia protetto da misure di sicurezza. Questa disposizione risulta presente esclusivamente in relazione alla perquisizione. Pertanto, tutte le volte in cui vi sarebbero delle barriere elettroniche da superare l'unico strumento valido sarebbe quello di cui all'art. 247 c.p.p.[10].

Da una diversa prospettiva, può farsi notare come ispezione, perquisizione e sequestro possano essere visti, in alcune situazioni, come atti posti in progressione[11]. Ci si riferisce ai casi in cui il sistema informatico oggetto di indagine sia particolarmente complesso, come nel caso dei *server* di una grande azienda. Acquisire mediante copia tutto il contenuto dei *server* costituirebbe un'operazione eccessivamente lunga e dispendiosa in termini di risorse. Per cui, si può facilmente immaginare una eventualità in cui un operante, in un primo momento ispezioni il sistema alla ricerca delle tracce del reato o degli effetti materiali dello stesso. In questa fase, pur con gli opportuni accorgimenti, il soggetto esplorerebbe il sistema senza andare alla ricerca di qualcosa di specifico. Tale operazione potrebbe trasformarsi successivamente in perquisizione allorché la rilevazione degli effetti materiali del reato possa

[9] Ancora, A. CISTERNA, *op. cit.*, pp. 66 s.

[10] Questa è la distinzione proposta da P. FELICIONI, *op. cit.*, pp. 146 s.

[11] In tal senso, S. ATERNO, *Art. 8*, in Cybercrime, *responsabilità degli enti e prova digitale* a cura di G. Corasaniti – G. Corrias Lucente, Cedam, Padova, 2009, p. 211.

condurre l'investigatore all'individuazione di dati o informazioni più rilevanti per l'indagine in corso. In questo caso, si passerebbe, senza soluzione di continuità, ad una perquisizione, il cui obiettivo sarebbe quello di rintracciare i dati informatici pertinenti al reato. Se l'operazione avesse esito positivo, verrebbero, infine, sequestrati solamente i documenti necessari o le porzioni del sistema informatico ritenuti utili per le indagini.

Al di là della delimitazione delle due fattispecie, deve essere sottolineato come il cuore dell'intervento legislativo effettuato tramite la l. n. 48/2008 sia stato quello di assicurare la genuinità del dato informatico raccolto attraverso gli atti di cui agli artt. 244, 247 c.p.p.[12]. Nel far ciò, il legislatore ha indicato l'obiettivo che deve essere perseguito dagli operanti senza, però, precisare le modalità di acquisizione e conservazione dei dati digitali. Sul punto la scelta, salutata con favore dalla dottrina, è stata quella di inserire una sorta di rinvio mobile alle c.d. *best practice* della *computer forensics*[13]. Infatti, sia l'art. 244 c.p.p. sia l'art. 247 c.p.p. fanno riferimento alla predisposizione di «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»[14].

Se questa è la strada che è stata scelta dal legislatore, occorre, tuttavia, porsi il problema di inquadrare giuridicamente tutte le fasi dell'attività di intervento da parte dell'autorità giudiziaria o della polizia giudiziaria, allorché emerga l'esigenza di raccogliere reperti di carattere informatico. Da un punto di vista generale, possono essere rilevati tre momenti

[12] V. P. FELICIONI, *op. cit.*, p. 233.

[13] Cfr. L. LUPÁRIA, Computer crimes *e procedimento penale*, in *Modelli differenziati di accertamento*, a cura di G. Garuti, in *Trattato di procedura penale*, diretto da G. Spangher, Utet, Torino, 2011, vol. VII, t. I, pp. 384 s. Sul

[14] Si registra in dottrina un dibattito circa l'individuazione della parte processuale gravata dall'onere di dover far emergere il mancato rispetto delle citate regole tecniche. A parere di F. CAJANI, *Il vaglio dibattimentale della* digital evidence, in *Arch. pen.*, 2013, pp. 851 s., sarebbe l'accusa a dover sempre dimostrare di aver rispettato le regole riguardanti le indagini informatiche. Questa, infatti, sarebbe obbligata a dar conto in dibattimento di tutte le operazioni svolte. Diversamente, F. GIUNCHEDI, *Le* malpractices *della* digital forensics. *Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *Arch. pen.*, 2013, p. 832 rileva come in un sistema accusatorio come quello disegnato dal codice di procedura penale dovrebbe essere la parte che intenda far uso di un determinato strumento a provare la sua corretta utilizzazione nel caso concreto.

differenti nell'acquisizione di dati informatici: l'individuazione del reperto, l'acquisizione del dato informatico e la sua analisi[15].

Per quanto riguarda il primo stadio della ricerca della prova di carattere informatico, ossia l'individuazione del reperto, questa si caratterizza per essere finalizzata alla ricerca dell'oggetto che potrebbe contenere informazioni rilevanti per le indagini preliminari. La positiva conduzione di tale fase non è per nulla scontata, ciò per almeno due ordini di ragioni. Da un lato, la costante miniaturizzazione delle memorie portabili può rendere particolarmente difficoltoso il ritrovamento di un tale dispositivo. Dall'altro lato, il numero di strumenti elettronici che sono in grado di collezionare informazioni rilevanti per un'inchiesta penale si amplia costantemente[16]. È necessario, in sostanza, che l'investigatore sia in grado di riconoscere tutti i *device* che potrebbero essere astrattamente utili alla ricostruzione del fatto[17]. L'attività posta in essere in questo momento iniziale assume, pertanto, natura ispettiva. L'organo requirente al fine di individuare il supporto contenente documenti rilevanti potrebbe dover, infatti, ispezionare tutti gli strumenti elettronici ritrovati sulla scena del crimine. Nello svolgimento di tale operazione, da compiersi attraverso gli opportuni *software* di *computer forensics*, l'investigatore si limita ad una generale visione del contenuto dello strumento informatico. Solo nel caso in cui, come prima precisato, si ponga la necessità di un controllo più approfondito, tale atto potrebbe trasformarsi in una perquisizione.

[15] Così, S. ATERNO, *op. cit.*, pp. 201 s.; P. FELICIONI, *op. cit.*, pp. 238 s.

[16] Cfr. l'elencazione fatta da P. BARILI, *Accertamenti informatici*, in *Le indagini scientifiche nel procedimento penale*, a cura di R.V.O. Valli, Giuffrè, Milano, 2013, p. 591.

[17] Se in un primo momento l'oggetto di analisi principale delle tecniche di cui si discute era il *computer*, deve essere rilevato come tale affermazione possa dirsi superata. Ormai un gran numero di strumenti di uso quotidiano è in grado di registrare informazioni utili per un investigatore. Si pensi ad uno *smartphone* o ad una *console* di videogiochi o, più in generale, agli oggetti cui si riferisce l'*Internet of things*. V. http://en.wikipedia.org/wiki/Internet_of_things

La fase di individuazione del reperto informatico può proseguire in due modalità differenti in relazione alla situazione di fatto che può presentarsi agli operanti.

Ci si riferisce, in particolare, alle situazioni in cui può diventare necessario compiere sin da questo momento, attività di c.d. *live forenics*, nel qual caso il sistema viene analizzato dagli operanti direttamente sul luogo in cui questo si trova. Le ragioni che potrebbero spingere gli investigatori al compimento di tali operazioni possono essere molteplici. In prima battuta, potrebbe capitare di trovare, sulla scena del crimine, un *computer* acceso. In questo caso, considerazioni di carattere tecnico ne sconsigliano lo spegnimento e il sequestro[18]. Inoltre, la complessità o la necessità di mantenere un determinato sistema informatico in funzione, potrebbero rendere nei fatti impraticabile un sequestro del supporto interessato dalle indagini.

In tali evenienze, in cui cioè l'attività di analisi e acquisizione dei dati segue direttamente quella di individuazione del reperto informatico, sarebbe necessario, secondo la dottrina, utilizzare lo strumento dell'accertamento tecnico irripetibile di cui all'art. 360 c.p.p.[19]. Tale istituto, infatti, permetterebbe, da un lato di garantire la genuinità del dato informatico analizzato e poi acquisito; e, dall'altro, grazie alla partecipazione della difesa, consentirebbe

[18] Il primo effetto che deriverebbe da uno spegnimento del dispositivo, sarebbe quello di cancellare la RAM La sigla è l'acronimo di *random-access memory*, per comprenderne l'importanza è utile una piccola digressione. Tendenzialmente ogni dispositivo elettronico è formato da una CPU (*Central processing Unit*), da una memoria principale e da una secondaria e, infine, da delle periferiche idonee a fornire *input* al sistema o a consegnare degli *output* all'utente. La CPU è l'unità che elabora le istruzioni che l'utente le fornisce; tuttavia, la stessa per lavorare ha bisogno di informazioni: queste sono immagazzinate nella memoria principale. La particolarità di quest'ultima è data dalla velocità di accesso ai dati in essa contenuti e dalla sua volatilità. Spento il sistema, le informazioni lì contenute vengono perse. Diversamente, la memoria secondaria consente un recupero più lento dei dati necessari alla CPU per lavorare, ma, a differenza della memoria principale, è in grado di mantenere memorizzati i dati anche quando il *computer* viene spento. In questo schema sommariamente delineato, la RAM è la memoria principale, mentre la memoria secondaria è rappresentata da *hard disk* o da *pendrive*. Per ulteriori chiarimenti, v. CHARLES SEVERANCE, *Python for informatics. Exploring Information*, pp. 1 ss., disponibile all'indirizzo http://www.pythonlearn.com

[19] Cfr. P. FELICIONI, *op. cit.*, p. 241

lo svolgimento di operazioni mirate finalizzate ad ottenere solo i dati e le informazioni necessarie alle indagini.

In tutte le altre eventualità, la naturale prosecuzione delle operazioni è data dal sequestro del supporto informatico rilevante per l'attività investigativa. Questo sarà in un secondo momento oggetto di copiatura al fine di poter permettere l'analisi forense dello stesso senza rischiare di danneggiare i dati originali[20]. L'obiettivo dell'analisi forense è, ovviamente, quello di estrarre dal supporto sequestrato il maggior numero di informazioni rilevanti per le indagini preliminari. In questa fase, diventa di fondamentale importante l'utilizzazione degli strumenti più adatti allo scopo. Pur non potendo giungere sino alla individuazione degli specifici *software* utilizzabili, deve rilevarsi come l'attività di analisi debba rispettare tre regole fondamentali. In primo luogo, devono essere salvaguardati al meglio i dati originali, il che impone di maneggiare il meno possibile il supporto originale e di compiere tutte le attività di analisi su una copia dello stesso. In secondo luogo, è fondamentale registrare con particolare cura tutte le operazioni che vengono svolte sul supporto analizzato. Tale requisito garantisce la trasparenza delle operazioni e permette alla difesa di poter ricostruire l'operato degli investigatori. In terzo luogo, le procedure utilizzate devono dirsi rispettose delle norme codicistiche.

Già durante la fase di ricerca dei dati informatici rilevanti, l'operato degli investigatori potrebbe essere bloccato dall'utilizzo, da parte dell'utilizzatore del *device* elettronico, di *password* o di strumenti di sicurezza tendenti a rendere impossibile la lettura e l'acquisizione dei dati. Sul punto, l'art. 247, co. 1 *bis* c.p.p. ammette la possibilità per gli investigatori di poter

[20] Sulla necessità dell'utilizzo della *bit-stream image* e sulle funzioni di *hash* v. Cap. II, § 2.

attivamente lavorare per disattivare tali misure di sicurezza[21]. Si tratta, con tutta evidenza, di un'autorizzazione da parte del legislatore a utilizzare strumenti di *hacking* sul dispositivo interessato. Tuttavia, alla luce della complessità che determinati sistemi di sicurezza possono avere (si pensi al caso in cui sia utilizzata una *passphrase*[22]), può talvolta diventare fondamentale la collaborazione dell'indagato proprietario del *device*. In questo caso, però, si aprono rilevanti scenari per lo studioso del processo penale.

Infatti può affermarsi che uno dei princìpi cardine cui è ispirato l'attuale codice di rito penale è quello espresso dal brocardo latino *nemo tenetur se detegere*, ossia della garanzia per l'imputato o indagato di non autoaccusarsi[23]. Tale impostazione è espressa da varie disposizioni del codice, tra cui, la più chiara sul punto è l'art. 64, co. 3° c.p.p. in materia di avvisi all'imputato allorché questi debba essere sottoposto ad interrogatorio. Si riconosce, infatti, il diritto dello stesso a rimanere in silenzio e a non collaborare con l'autorità. Non solo, il principio in discorso costituisce, come messo in luce da parte della dottrina, uno dei profili sottesi all'art. 188 c.p.p. in tema di autodeterminazione delle persone coinvolte nel procedimento

[21] Sul punto merita quantomeno di essere citata la vicenda che ha visto contrapposti la *Apple Inc.* all'*F.B.I.* Punto della discussione era proprio la collaborazione della società californiana con le autorità al fine di disattivare le misure di sicurezza di un *iphone* di proprietà di un terrorista. La richiesta principale dell'*F.B.I.* era quella di ottenere da *Apple* una versione modificata dal *software iOS* che permettesse alle autorità di aggirare i sistemi di sicurezza attivati dal terrorista. Nonostante un ordine impartito dalla Corte distrettuale della California, la *Apple*, pubblicamente, si è rifiutata di cooperare con gli investigatori. L'argomentazione centrale fatta propria dal colosso dell'*hi-tech* è incentrata sul pericolo che deriverebbe per la *privacy* dei suoi clienti, nel caso in cui venisse effettivamente rilasciato un tale *software*. L'episodio si è positivamente concluso grazie all'intervento della *N.S.A.*, la quale è stata in grado di "sbloccare" l'*iphone* oggetto di indagine mettendolo così a disposizione dell'*F.B.I.* La vicenda, dagli innumerevoli risvolti interessanti, renderebbe in un certo senso evidente l'ingenuità del legislatore italiano del 2008, il quale sembrerebbe configurare l'operazione di superamento delle misure di sicurezza dei dispositivi elettronici come un'operazione di *routine* per gli esperti di *computer forensics*.

[22] La differenza principale tra *password* e *passphrase* è data dalla lunghezza dei caratteri utilizzati, mentre la prima è formata da 6/8 caratteri, la seconda è costituita da almeno 20/30 caratteri. Più alto è il numero di caratteri utilizzati, più diventano difficili, fino a diventare impossibili, i c.d. attacchi a forza bruta. Con questa espressione si fa riferimento all'utilizzo di *software* in grado di provare tutte le possibili combinazioni di caratteri, fino a scoprire quella che consente l'ingresso nel sistema. V. http://en.wikipedia.org/wiki/Brute-force_attack

[23] Per alcuni approfondimenti sul tema, si rimanda a V. GREVI, Nemo tenetur se detegere*: interrogario dell'imputato e diritto al silenzio nel processo penale italiano*, Giuffrè, Milano, 1972, *passim*. Più recentemente, v. V. PATANÈ, *Il diritto al silenzio dell'imputato*, Giappichelli, Torino, 2006, *passim*.

penale[24]. Infatti uno dei riflessi del diritto ad autodeterminarsi è, sicuramente, rappresentato dal diritto a non collaborare.

In questo quadro normativo si inserisce la questione circa la sussistenza o meno per l'imputato di un obbligo di consegna della *password*. Per una parte della dottrina, un tale obbligo non sarebbe configurabile proprio in ragione del principio del *nemo tenetur se detegere*. Questo è, infatti, un valore fondamentale del nostro ordinamento processuale che dà concretezza a numerosi princìpi espressi dalla Costituzione, come il riconoscimento dei diritti inviolabili della persona e il diritto di difesa[25]. Seguendo tale linea di pensiero, si giunge a ritenere necessario per gli operanti di avvisare l'indagato, *ex* art. 64, co. 3° c.p.p., del suo diritto al silenzio prima di chiedere la collaborazione di quest'ultimo. Non solo: stando sempre a tale ricostruzione, allorché non fosse dato l'avviso di cui all'art. 64, co. 3°, lett. *b*) c.p.p., si presenterebbe un'ipotesi di inutilizzabilità derivata. Infatti l'inutilizzabilità della dichiarazione dell'indagato discendente dall'applicazione dell'art. 64, co. 3 *bis* c.p.p., si riverberebbe sul materiale informatico ottenuto grazie alla collaborazione dello stesso[26]. Discorso non dissimile dovrebbe essere compiuto per chiunque, pur non essendo indagato, non voglia fornire le chiavi di accesso ad un sistema informatico, temendo che da tale operazione possa emergere una sua responsabilità penale. In questo caso, la disposizione di riferimento sarebbe costituita dall'art. 198, co. 2° c.p.p.[27].

---

[24] Cfr. V. GREVI, *op. cit.*, pp. 67 s.; O. MAZZA, *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, Giuffré, Milano, 2004, pp. 36 s.

[25] Più correttamente, la dottrina riconduce il principio in discorso alla tutela dei diritti compresi negli artt. 2, 13, 24, 27, 111 Cost. Sul punto, v. L. LUPÁRIA, *La disciplina processuale e le garanzie difensive*, in *Investigazione penale e tecnologia informatica*, a cura di L. Lupária – G. Ziccardi, Giuffrè, Milano, 2007, p. 159.

[26] In tal senso si esprimono, L. LUPÁRIA, *La disciplina*, cit., p. 160; L. MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 3516, il quale, inoltre, ritiene che nemmeno inquadrando la dichiarazione dell'indagato che fornisce la *passoword* tra quelle di cui all'art. 350, co. 6° c.p.p. vi potrebbe essere una salvaguardia del diritto di difesa dello stesso. Infatti, pur rimanendo completamente inutilizzabile come dichiarazione, questa potrebbe orientare in senso decisivo le indagini.

[27] V. ancora, L. LUPÁRIA, *La disciplina*, cit., p. 160.

In senso opposto, un'altra parte della dottrina, pur riconoscendo l'importanza del diritto a non collaborare da parte dell'indagato o imputato, rileva come l'avviso di cui all'art. 64, co. 3°, lett. *b*) c.p.p. sia previsto non per qualsiasi atto cui la persona sottoposta a procedimento penale debba partecipare, ma solo per quelli in cui questi interviene, non volontariamente, come dichiarante[28].

Una linea argomentativa possibile per risolvere la questione potrebbe essere quella di richiamare le considerazioni svolte dalla dottrina in tema di ricognizioni[29]. Infatti è ampiamente discusso tra gli studiosi e in giurisprudenza, fin dove possa spingersi il diritto di non collaborare allo svolgimento dell'atto da parte dell'imputato. Ricostruendo sommariamente il dibattito citato, si può affermare come il nodo centrale della questione riguardi il comportamento tenuto dall'imputato. In questo senso, si differenziano le situazioni in cui il soggetto debba assumere, rispetto all'atto probatorio un ruolo attivo, da quelle in cui lo stesso assuma dei comportamenti di carattere passivo. Nel primo caso, non vi sarebbe alcuna possibilità per l'autorità procedente di coartare la volontà del soggetto. Un eventuale intervento in tal senso costituirebbe sicuramente una violazione dell'art. 188 c.p.p., comportando l'inutilizzabilità della prova così ottenuta.

Il diritto di non collaborare viene meno, però, allorché l'imputato non sia il soggetto della prova, ma ne sia l'oggetto come nel caso di una ispezione o una ricognizione personale.

[28] P. FELICIONI, *op. cit.*, pp. 247 s.

[29] Per una più ampia analisi dell'istituto delle ricognizioni, v. F. M. PAOLA, *Ricognizioni*, in *Dig. pen.*, Utet, Torino, 1997, vol. XII, pp. 218 ss.; P. MOSCARINI, *Ricognizione (proc. pen.)*, in *Enc. giur. Treccani*, 1994, pp. 1 ss.

In questo caso, l'autorità procedente può prendere provvedimenti di carattere coercitivo al fine di neutralizzare la condotta ostruzionistica dell'indagato o imputato[30].

Alla luce di queste considerazioni, si può provare a rispondere al quesito sopra posto sulla base di un ragionamento di carattere analogico. Considerando che l'estensione del diritto di non collaborare da parte dell'imputato copre anche tutte le dichiarazioni dello stesso, in quanto comportamenti di carattere attivo, si può ritenere come un eventuale tentativo da parte dell'autorità procedente di coartare la volontà del soggetto per ottenere le chiavi di sicurezza dello strumento elettronico costituisca una violazione dell'art. 188 c.p.p., con tutte le conseguenze già prima delineate.

[30] Si tratta, ovviamente, di provvedimenti di carattere eccezionale che dovranno necessariamente indicare con precisione gli atti che possono essere compiuti, in modo da garantire che gli stessi siano limitati ai soli comportamenti che possano rendere possibile l'atto ricognitivo. V., sul punto, P. FERRUA, *Sulla legittimità della ricognizione compiuta contro la volontà dell'imputato*, in *Cass. pen.*, 1990, I, p. 653.

2. Il sequestro di materiale informatico

Al fine di una compiuta ricostruzione dei punti critici del sequestro di materiale informatico, risulta utile una breve ricostruzione dei tratti salienti del mezzo di ricerca della prova regolato dagli artt. 253 ss. c.p.p. Il termine «sequestro» fa generalmente riferimento all'apposizione di un vincolo di indisponibilità su di un oggetto determinato. Come riconosciuto dalla dottrina, il provvedimento dell'autorità giudiziaria, emanato per finalità di carattere probatorio, va a ledere almeno due beni giuridici di valore costituzionale: il diritto di proprietà e quello della libertà di iniziativa economica[31]. Sulla base di tale nozione generale è stato disegnato l'istituto del sequestro[32].

Il sequestro probatorio, inserito non a caso nel capo III del titolo III del libro III del codice di rito penale, svolge la funzione di garantire che le cose necessarie per l'accertamento del reato siano opportunamente conservate. Da tale affermazione, si evidenzia un ulteriore profilo riguardante il sequestro di materiale probatorio, ossia quello cautelare[33]. Infatti non è estranea alla *ratio* dell'atto in discorso l'idea di garantire che la cosa sottoposta a vincolo di

[31] Cfr., *ex multis*, F. M. GRIFFANTINI, *Riesame del sequestro e valutazione dei presupposti nella giurisprudenza sul c.p.p. 1930 e nel c.p.p. del 1988* in *Riv. it. dir. proc. pen.*, 1990, p. 164; E. SELVAGGI, *Artt. 253-265*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. II, p. 751.

[32] Allo stato, nel codice di rito penale esistono tre tipologie di sequestro: quello probatorio, quello preventivo e quello conservativo. Solo il primo ha, come meglio si vedrà, finalità attinenti alla ricerca della prova. Gli altri due condividono obiettivi di natura cautelare: il sequestro preventivo mira ad evitare che la disponibilità di una determinata cosa possa aggravare le conseguenze del reato; viceversa, il sequestro conservativo svolge la funzione di evitare che il patrimonio dell'imputato si riveli incapiente al momento del pagamento della pena pecuniaria o delle spese processuali. Per alcune nozioni di ampio respiro sull'istituto del sequestro, si rimanda a M. MONTAGNA, *Sequestri*, in *Dig. pen.*, Utet, Torino, 2005, agg. III, pp. 1543 ss. Più nello specifico in relazione al sequestro come misura cautelare reale v. M. FERRAIOLI, *Misure cautelari*, in *Enc. giur. Treccani*, 1990, pp. 20 ss.; A. M. DE SANTIS, *Sequestro preventivo*, in *Dig. pen.*, Utet, Torino, 1997, vol. XIII, pp. 264 ss.; E. SELVAGGI, *Art. 312*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. IV, pp. 360 ss.; E. SELVAGGI, *Art. 316*, in *Commento*, cit., pp. 332 ss. N. VENTURA, *Sequestro preventivo*, in *Dig. pen.*, Utet, Torino, 2004, agg. II, pp. 750 ss.

[33] V., in tal senso, U. DE CRESCIENZO, *Il sequestro penale e civile*, Utet, Torino, 1997, p. 6; E. SELVAGGI, *Artt. 253-265*, cit., p. 736.

indisponibilità non sia distrutta, alterata o, comunque, resa inutilizzabile ai fini dell'accertamento del fatto di cui all'imputazione nel momento in cui sia celebrato il processo.

L'oggetto del sequestro è indicato *per tabulas* dal legislatore all'art. 253, co. 1° c.p.p., laddove stabilisce la possibilità di disporre il sequestro «del corpo del reato e delle cose pertinenti al reato necessarie per l'accertamento dei fatti». Dal canto suo, la dottrina ha posto in luce la natura tassativa dell'indicazione relativa all'oggetto del sequestro di cui alla disposizione citata[34]. Il ragionamento deriva dal corretto inserimento del sequestro nella sistematica dei mezzi di ricerca della prova. Partendo dall'idea per cui gli atti di natura probatoria che, coinvolgendo direttamente l'individuo, vanno ad incidere direttamente sui diritti fondamentali dello stesso sono da considerarsi tassativi, consegue che anche la normativa in tema di sequestro, in quanto quest'ultimo è strumento di carattere coercitivo che lede beni giuridici protetti dalla Costituzione, sia da interpretare in senso restrittivo[35].

Per quanto attiene alla nozione di corpo del reato, il legislatore ha sentito la necessità di darne una definizione all'interno dell'art. 253, co. 2° c.p.p. Per corpo del reato devono intendersi « le cose sulle quali o mediante le quali il reato è stato commesso nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo»[36]. La dottrina, dal canto suo, ha sottolineato come il concetto di corpo del reato possa essere scomposto in due elementi: uno materiale, ossia la cosa cui fa riferimento il termine «corpo» e uno relazionale, ossia il rapporto sussistente tra l'oggetto e il fatto che deve essere accertato[37].

---

[34] Cfr. G. JESU, *Inaccettabili approdi in tema di sequestro probatorio*, in *Cass. pen.*, 1999, pp. 1080 s.; G. TRANCHINA, *Sequestro II) sequestro penale*, in *Enc. giur. Treccani*, Roma, 1994, p. 2.

[35] Posizione che trova riscontro anche in Corte cost., 19 giugno 1998, n. 229, in *Giur. cost.*, 1998, pp. 1786 ss., nella quale si afferma espressamente che il sequestro di ciò che non è corpo del reato o cosa pertinente al reato sia da considerare illegittimo.

[36] La necessità di fornire una tale definizione era sorta sulla base dell'eccessiva dilatazione della stessa durante la vigenza del codice del 1930. Per quanto riguarda la definizione di prodotto, profitto e prezzo del reato è utile un rimando a Cass. sez. Un., 3 luglio 1996, Chabni Samir, in *C.e.d. cass.* n. 205707.

[37] Così, C. U. DEL POZZO, *Corpo del reato* in *Enc. dir.*, Giuffrè, Milano, 1962, vol. X, p. 650.

Diversamente, l'elaborazione del concetto di cosa pertinente al reato è stata lasciata all'opera della dottrina e della giurisprudenza. Questi hanno ricostruito tale nozione sulla base della funzione che un determinato oggetto può svolgere in relazione all'illecito penale che deve essere accertato. La cosa pertinente al reato si caratterizza per essere qualsiasi oggetto dotato di una sua idoneità all'accertamento del fatto. Ciò che diviene rilevante non è, quindi la natura dell'oggetto, ma il suo rapporto col procedimento; come affermato da un'autorevole dottrina, è cosa pertinente al reato ogni reperto che sia utile alla decisione[38].

Alla luce di tali premesse, si discute in dottrina circa la possibilità di effettuare un sequestro di beni immateriali. Secondo una ricostruzione risalente al codice di procedura penale del 1930, tale tipologia di oggetti non sarebbe sottoponibile al vincolo tipico del sequestro. Tale affermazione trovava riscontro nel testo della normativa in tema di sequestri, laddove si faceva riferimento espresso alla consegna della cosa al custode[39]. In riferimento al codice di rito vigente, alcuni Autori hanno ritenuto ancora valida l'impostazione riferita[40].

In seno a tale orientamento, vi è chi ha sviluppato alcune precisazioni riguardanti l'incorporeità del bene sequestrabile. Secondo questi studiosi, il corpo del reato non potrebbe mai essere un'entità immateriale in quanto il concetto stesso di «corpo del reato» presupporrebbe la sussistenza, appunto, di una corporeità. Soltanto le cose pertinenti al reato potrebbero essere prive di dimensione materiale[41].

[38] Così, F. CORDERO, *op. cit.*, p. 837.

[39] Cfr. A. AMODIO, *Dal sequestro in funzione probatoria al sequestro preventivo: nuove dimensioni della «coercizione reale» nella prassi e nella giurisprudenza*, in *Cass. pen.*, 1982, p. 1076.

[40] Ci si riferisce a F. CORDERO, *op. cit.*, p. 837; A. MELCHIONDA, *Sequestro (dir. proc. pen.)*, in *Enc. dir.*, Giuffrè, Milano, 1990, vol. XLII, p. 150.

[41] In tali termini, v. R. CANTONE, *Perquisizioni e sequestri: dalle tecniche investigative alle problematiche processuali*, in *Arch. n. proc. pen.*, 2001, p. 7; A. NAPPI, *Guida al codice di procedura penale*, Giuffrè, Milano, 10° ed., 2007, p. 308.

Già dalla delimitazione dell'oggetto del sequestro emergono quelli che sono i presupposti dell'atto. In primo luogo, il sequestro può essere disposto soltanto successivamente alla ricezione di una notizia di reato. È esclusa qualsiasi possibilità di utilizzo dello strumento in discorso per finalità di carattere esplorativo o di acquisizione della notizia di reato. Tuttavia, è dibattuto, soprattutto in giurisprudenza il livello di approfondimento della *notitia criminis* che possa giustificare tale atto.

Da un lato, alcune pronunce della Corte di cassazione, sostenendo un'impostazione di carattere restrittivo, riconoscono la legittimità del provvedimento di sequestro solo allorché la fattispecie di reato sia individuata con sufficiente precisione[42]. Dall'altro, un secondo orientamento, di stampo estensivo, ne ammette la possibilità quando sussista anche soltanto l'astratta configurabilità della commissione di un reato[43].

Sul punto, è intervenuta nei primi anni di vigenza del codice di procedura penale un'importante pronuncia della Corte di cassazione a Sezioni Unite[44]. Questa ha scelto una strada che potrebbe definirsi mediana rispetto alle due opzioni interpretative riferite: infatti connaturata all'idea stessa di corpo del reato o di cosa pertinente al reato è la commissione di un illecito penale. Da ciò, deriva che uno dei presupposti del decreto di sequestro è rappresentato dalla sussistenza di un *fumus commissi delicti*. Tale espressione sarebbe da intendere come un'ipotesi di reato che sia «ascrivibile alla "realtà effettuale" e non a quella "virtuale"[45]».

[42] Cfr. Cass. sez. I, 3 ottobre 1997, Attaniese, in *C.e.d. cass.* n. 209889; Cass. sez. III, 25 febbraio 2003, Conventi, in *C.e.d. cass.* n. 224882.

[43] Cfr. Cass. sez. V, 8 febbraio 1999, Circi, in *C.e.d. cass.* n. 212778; Cass. sez. III, 10 marzo 2015, Previtero, in *C.e.d. cass.* n. 263053.

[44] Cfr. Cass. sez. Un., 20 novembre 1996, Bassi ed altri, in *C.e.d. cass.* n. 206657.

[45] Cfr. Cass. sez. Un., 20 novembre 1996, Bassi ed altri, cit. In questo contesto è l'autorità giurisdizionale che deve controllare in sede di riesame del sequestro la congruità degli elementi utilizzati dalla pubblica accusa per giustificare il provvedimento ablativo. Il giudice in questa eventualità si muove su un delicato crinale: da un lato non

Nel quadro brevemente tratteggiato si inserisce la particolare tematica del sequestro di materiale informatico, operazione che si pone sotto certi aspetti in frizione con i tradizionali elementi che contraddistinguono il sequestro probatorio.

Questione di primaria importanza tra quelle da affrontare è quella riguardante proprio l'oggetto del sequestro. Qualora l'illecito sia ricompreso nei c.d. *computer crimes*, è altamente probabile che il *device* elettronico costituisca il corpo del reato oppure cosa pertinente al reato. In tali casi, infatti, lo strumento elettronico è stato il mezzo attraverso cui è stato perpetrato l'illecito ed è, in quanto tale, pacificamente qualificabile come corpo del reato. Diverso è il caso in cui lo strumento elettronico non sia nella sua interezza elemento utile alla ricostruzione dei fatti, ma contenga, in realtà, informazioni rilevanti per l'indagine penale. In questa eventualità si apre l'importante questione riguardante l'estensione del provvedimento di sequestro.

Si potrebbe ritenere che anche in questa ipotesi sia legittimo sequestrare l'intero sistema informatico. Tuttavia, una tale affermazione risulta criticabile sotto più punti di vista.

In primo luogo, questione centrale per lo studioso del processo penale, un provvedimento del genere si qualificherebbe per il fatto di comportare una sproporzionata lesione di beni fondamentali protetti sia dalla Costituzione sia dalle Carte dei diritti di livello europeo e internazionale[46]. Il riferimento non è tanto alla limitazione del diritto di proprietà – profilo, comunque, non irrilevante – ma, più precisamente, alla tematica afferente al diritto alla riservatezza degli individui. Come ripetuto più volte durante la trattazione, lo strumento informatico è ormai un contenitore di informazioni estremamente personali, le quali meritano

può instaurare un processo nel processo per verificare la piena fondatezza dell'ipotesi accusatoria, ma dall'altro lato non può limitarsi ad accettare acriticamente la ricostruzione dei fatti presentati dal magistrato requirente.

[46] V. Cap. III per uno studio delle posizioni giuridiche soggettive lese dagli atti di *digital forensics*.

di essere protette da interventi arbitrari dell'autorità procedente[47]. Non solo, l'acquisizione generica di tutto il contenuto di un sistema elettronico comporterebbe l'alto rischio di vedere trasformato il sequestro probatorio da mezzo di ricerca della prova a strumento di individuazione della notizia di reato[48]. Il discorso mantiene tutta la sua validità anche quando dal *device* venga estratta fisicamente la memoria su cui sono salvati tutti i dati dell'utente, come avviene nel caso di sequestro di *hard disk*.

In secondo luogo, come rilevato dalla dottrina, la stessa sussunzione del *computer* sotto la categoria di corpo del reato o di cosa pertinente al reato è ampiamente discutibile. Infatti, precisa questa impostazione, l'elaboratore elettronico è un oggetto comune, privo di particolari caratteristiche che, all'interno di un'indagine penale, svolge esclusivamente la funzione di contenitore occasionale di informazioni rilevanti. A meno che lo stesso non sia stato utilizzato attivamente per la commissione dell'illecito penale, difficilmente potrebbe essere sottoposto a sequestro probatorio a norma dell'art. 253 c.p.p.[49].

In terzo luogo, si possono presentare situazioni in cui non sia possibile disporre il sequestro del sistema. Esemplificando, il sequestro di tutto il sistema informatico di una grande azienda potrebbe presentare delle difficoltà tutt'altro che aggirabili.

Queste argomentazioni potrebbero spingere a preferire una diversa soluzione, ossia quella di circoscrivere il sequestro ai soli dati informatici in quanto tali, separando, pertanto, il contenitore dal contenuto. Tuttavia, non mancano voci in dottrina che, riallacciandosi

[47] Sul principio di proporzionalità si rimanda alle considerazioni di M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont.*, 2014, nn. 3-4, pp. 143 ss.

[48] Questione affrontata da Cass. sez. IV, 17 aprile 2012, p.m. in c. soc. Ryanair, in *C.e.d. cass.* n. 252689.

[49] Ci si riferisce alle argomentazioni di A. CHELO MANCHÌA, *Sequestro probatorio di* computers*: un provvedimento superato dalla tecnologia?* in *Cass. pen.*, 2005, p. 1635.

all'orientamento prima riferito, sottolineano come l'incorporeità del dato digitale sembrerebbe escluderne la possibilità di sequestro[50]. In realtà, si potrebbe replicare a tali obiezioni sottolineando come i dati informatici abbiano una loro, benché minima, corporeità trattandosi di impulsi elettromagnetici registrati su di un supporto fisico. Questi sono suscettibili di apprensione, seppur con tecniche particolari. Come specificato da autorevole dottrina, il documento informatico più che immateriale è dematerializzato[51].

Di più difficile soluzione è la questione concernente l'estensione del provvedimento di sequestro. Nella prassi il sequestro di dati informatici passa ordinariamente attraverso la copiatura integrale dell'*hard disk* e la successiva restituzione dello stesso al legittimo proprietario[52]. Questa è generalmente ritenuta la soluzione migliore anche dal punto di vista delle buone pratiche di *computer forensics*[53]. L'effettuazione di una copiatura integrale attraverso lo strumento della *bitstream image* permettendo la ricostruzione di un *hard disk* in tutto e per tutto uguale, dal punto di vista logico, a quello sottoposto a sequestro sembra essere per molti studiosi la soluzione più adatta. In realtà, sarebbe più opportuno valorizzare le opzioni interpretative indicate dalla già citata l. n. 48/2008, la quale può fornire utili spunti in proposito[54]. Primo fra tutti, la piena valorizzazione della funzione di ricerca della prova della perquisizione informatica. Questa, come atto idoneo a permettere una prima osservazione del

[50] Ancora A. CHELO MANCHÌA, *op. cit.*, pp. 1635 s. Più recentemente, V. ZAMPERINI, *Impugnabilità del sequestro probatorio di dati informatici*, in *Dir. pen. proc.*, 2016, p. 515.

[51] V. Cap. II, § 2.

[52] Come segnalato da, P. TROISI, *Sequestro probatorio del* computer *e segreto giornalistico*, in *Dir. pen. proc.*, 2008, p. 767, nt. 10 qualora il supporto sequestrato contenga materiale illecito, si pensi ai casi detenzione di materiale pedopornografico, il sequestro probatorio dovrebbe convertirsi in sequestro preventivo. Più articolata la soluzione proposta da A. CHELO MANCHÌA, *op. cit.*, pp. 1637 ss., il quale ritiene possibile la restituzione dell'*hard disk* ma soltanto dopo aver opportunamente cifrato i dati di carattere illecito. In tale ricostruzione, che ha sicuramente il pregio di garantire il diritto del proprietario a non vedersi sottratto il *device* elettronico, questi riacquisterebbe la piena disponibilità del materiale sequestrato soltanto al termine del processo quando, in caso di esito favorevole del processo, gli verrebbero consegnate le chiavi crittografiche.

[53] V. Cap. II, § 1, nt. 12.

[54] Il tema del sequestro di dati presso i fornitori di connettività sarà trattato successivamente nella trattazione.

sistema informatico, può, infatti, permettere la predisposizione di un atto maggiormente mirato[55].

Dal canto suo, la giurisprudenza si è resa conto della complessità del tema ed ha proposto alcune soluzioni. In particolare, le pronunce che più si sono occupate di tale argomento hanno riguardato la complessa questione del sequestro di materiale informatico di proprietà di un giornalista. La questione presenta più profili di interesse, in quanto coinvolge anche il delicato equilibrio sussistente tra il diritto del giornalista a non rilevare il nome delle sue fonti e quello all'accertamento dei fatti di reato.

In una risalente pronuncia, seguita poi dalla giurisprudenza successiva, i giudici di legittimità hanno riconosciuto la sussistenza di un particolare obbligo di motivazione in capo al giudice che dispone il sequestro, in modo che l'oggetto dello stesso possa essere individuato con precisione[56]. Come rilevato dalla dottrina che ha commentato tale arresto giurisprudenziale, ciò che deve essere precisato all'interno del decreto di sequestro deve essere la connessione tra il *thema probandum* e l'attività di ricerca dei mezzi di prova[57].

---

[55] Sulle ipotesi *de jure condito* e *de jure condendo* si avrà modo di ritornare più avanti nel prosieguo del lavoro.

[56] Cfr. Cass. sez. I, 16 febbraio 2007, Pomarici, in *C.e.d. cass.* n. 257555 nonché in *Cass. pen.*, 2008, pp. 2946 ss. con nota di A. LOGLI, *Sequestro probatorio di un* personal computer. *Misure* ad explorandum *e tutela della corrispondenza elettronica.* La vicenda si inserisce nella complicata indagine nata dal rapimento dell'imam Abu Omar: durante tale procedimento erano state pubblicate sulla stampa periodica alcuni stralci di verbali di atti coperti da segreto istruttorio. L'attività inquirente ha condotto, dopo vari passaggi, a sospettare che un giornalista, diverso da quello che aveva pubblicato gli atti citati, avrebbe potuto essere in diretto contatto con la fonte confidenziale che aveva diffuso i verbali poi pubblicati. Per questo motivo, veniva sequestrato il *computer* del giornalista, effettuata una copia integrale tramite le modalità della *bitstream image* dell'*hard disk* del sistema sequestrato e restituito lo stesso al legittimo proprietario. La Corte di cassazione in sede di impugnazione a seguito di riesame del provvedimento di sequestro ne ha sottolineato l'illegittimità a causa della genericità della motivazione. I giudici di legittimità censurano il provvedimento emanato a causa del rischio che lo stesso avesse una finalità di carattere esplorativo più che acquisitivo. Per un generale riassunto della vicenda, si rimanda alla precisa ricostruzione contenuta in Corte eur., 23 febbraio 2016, Nasr e Ghali c. Italia §§ 8 ss. e commentata da A. LIGUORI, Extraordinary Redentions *nella giurisprudenza della Corte europea dei diritti umani: il caso Abu Omar*, in *Riv. dir. int.*, 2016, pp. 777 ss. Successivamente alla pronuncia in oggetto, la Corte di cassazione ha ribadito più volte il suo orientamento sul punto, v. Cass. sez. VI, 31 maggio 2007, Sarzanini, in *C.e.d. cass.* n. 237917; Cass. sez. II, 9 dicembre 2011, Massari, in *C.e.d. cass.* n. 252054; Cass. sez. VI, 15 aprile 2014, Minniti ed altro, in *C.e.d. cass.* n. 260068; Cass. sez. VI, 24 febbraio 2015, Rizzo, in *C.e.d. cass.* n. 264094.

[57] Cfr. A. LOGLI, *op. cit.*, p. 2955.

Sempre secondo questi studiosi, sarebbe proprio l'attività stessa di copiatura attraverso *bitstream image* a presentare profili problematici. Sarebbe, infatti, l'effettuazione di una copia completa del supporto in cui sono memorizzati i dati informatici a far svanire i confini tra attività di ricerca della notizia di reato, da un lato, considerata illecita se compiuta attraverso un sequestro e, attività acquisitiva di materiale probatorio, dall'altro[58].

Un tale orientamento deve essere, però, calato nella realtà concreta delle eventualità che gli investigatori potrebbero trovarsi ad affrontare. Il pensiero va al caso in cui si ritenga necessario lo svolgimento di un'attività di analisi approfondita del supporto informatico tesa a recuperare anche quei *files* o quei frammenti di dati che il singolo potrebbe aver cancellato o, comunque, tentato di celare[59].

In definitiva, non sarebbe corretto valutare come incondizionatamente illegittima l'acquisizione tramite copia forense dell'intero supporto informatico. Appare al contrario, opportuno distinguere se dalle risultanze investigative emergono elementi tali da ritenere che informazioni utili alle indagini preliminari siano nascoste all'interno dell'elaboratore, allora la strada della copia forense è sicuramente la più opportuna, purché l'autorità giudiziaria sia in grado di motivare adeguatamente sul punto. Viceversa, allorché si vada alla ricerca di materiale ben specifico senza che si possa inferire dall'attività inquirente condotta che vi sia la necessità di effettuare particolari operazioni sull'*hard disk*, allora non appare corretto procedere all'integrale copiatura del supporto[60].

Altra tematica strettamente connessa con il sequestro di materiale probatorio è quello della custodia del supporto sottoposto a vincolo di indisponibilità. Sul punto è intervenuto

[58] V., ancora, A. LOGLI, *op. cit.*, p. 2956.

[59] Cfr. P. TROISI, *op. cit.*, p. 767.

[60] L'esempio classico di tale eventualità è proprio quella in cui il *computer* o il *device* elettronico siano di proprietà di un soggetto estraneo all'indagine, il quale può, tutt'al più fornire elementi utili per la stessa.

direttamente il legislatore attraverso la già citata l. n. 48/2008 con cui è stata data esecuzione alla Convenzione di Budapest. L'opera del legislatore si è tradotta nell'interpolazione degli artt. 259, 260 c.p.p.

Sono stati, anzitutto, introdotti nuovi obblighi in capo al custode del materiale sequestrato tendenti a garantire la genuinità del dato informatico. In particolare è stato previsto che «quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria». La dottrina ha sottolineato come si tratti di una mera precisazione di quanto già si poteva inferire dal previgente testo normativo[61]. Infatti l'idea che la cosa sequestrata debba essere conservata in modo da evitarne l'alterazione è connaturata al concetto stesso di custodia: per cui, indipendentemente dalla modifica legislativa, graverebbe sul custode l'obbligo di evitare qualsiasi tipo di contaminazione dei dati informatici[62].

Più significative risultano, invece, le modifiche apportate all'art. 260 c.p.p. È stata, in primo luogo, prevista la possibilità di apporre sigilli di carattere anche elettronico al materiale sequestrato. Trovano in questa maniera ingresso *per tabulas* quei meccanismi di validazione della prova compiuti attraverso le funzioni di *hash*[63]. Inoltre, viene *ex novo* stabilito che la copia del materiale sia effettuata attraverso l'impiego di metodologie che ne garanti-

[61] V., L. CORDÌ, *Commento all'art. 8 l. 18 marzo 2008, n. 48*, in *Leg. pen.*, 2008, p. 296; L. LUPÁRIA, *La ratifica*, cit., p. 721.

[62] In tal senso, L. CORDÌ, *op. cit.*, p. 296.

[63] Sul punto, si richiamano le considerazioni di cui al Cap. II, § 1.

scano l'identità con l'originale e l'uso di supporti adeguati. Il legislatore sembra aver confermato anche in tema di sequestro la volontà di far entrare nel nostro ordinamento le c.d. *best pratice* della *digital forensics*[64].

Da un punto di vista operativo viene suggerita dalla dottrina l'idea per cui la conservazione del reperto informatico debba rifarsi al principio della c.d. continuità probatoria, ossia all'idea per cui tutta l'attività di repertazione e conservazione dell'elemento di prova debba essere tracciata. In quest'ottica, risulta, ovviamente, di capitale importanza la catena di custodia[65]. L'espressione con la quale si fa riferimento alla completa documentazione delle operazioni compiute sul supporto[66].

L'ultima tematica da affrontare in tema di sequestro di dati informatici ha per oggetto l'ammissibilità del riesame del provvedimento ablativo allorché il supporto sia stato restituito al soggetto indagato ma sia stata trattenuta dall'autorità giudiziaria copia integrale dei dati memorizzati sullo stesso.

Partendo da alcune considerazioni di carattere generale, va ricordato come l'art. 257 c.p.p. ammetta la possibilità in capo sia all'imputato sia a chi avrebbe diritto alla restituzione della cosa di proporre riesame del decreto di sequestro. Come rilevato dalla dottrina, la *ratio* di una tale previsione sta nella necessità di assicurare che anche i provvedimenti in discorso siano emanati nel rispetto della normativa codicistica, esigenza questa che deriva direttamente dal fatto che attraverso il sequestro l'autorità giudiziaria va a ledere beni di sicura rilevanza costituzionale[67]. In merito ai soggetti legittimati, come accennato, l'art. 257 c.p.p. fa

[64] L. CORDÌ, *op. cit.*, p. 296 sottopone a critica la distinzione tra originale e copia quando si fa riferimento ai dati informatici sottoposti a sequestro.

[65] Cfr. M. MATTIUCCI – G. DELFINIS, Forensic Computing, in *Rass. Arm. Carabinieri*, 2006, 2, p. 66, nt. 8.

[66] V., P. FELICIONI, *op. cit.*, p. 236.

[67] Così, G. TRANCHINA, *op. cit.*, p. 6; E. SELVAGGI, *Artt. 253-265*, cit., p. 751.

riferimento non soltanto all'imputato, cui è equiparata *ex* art. 61 c.p.p. anche la persona sottoposta alle indagini, ma anche chi possa vantare un diritto di proprietà sulla cosa oggetto di sequestro.

Oggetto di acceso dibattito, tanto in dottrina quanto in giurisprudenza è la questione concernente l'interesse ad impugnare il provvedimento di sequestro allorché, acquisita la copia, sia stato restituito il supporto originale. In prima battuta pare potersi affermare come l'interesse sotteso all'impugnazione dello stesso sia quello connesso alla restituzione del bene e al ripristino del pieno potere sulla cosa da parte del legittimo proprietario. Di conseguenza, la restituzione della cosa farebbe venir meno qualsiasi interesse a coltivare l'impugnazione.

La situazione risulta, però, più complessa allorché, appunto, venga effettuata una copia di ciò che è stato sequestrato e ad essere restituito sia il solo documento originale. Infatti in tale evenienza sembrerebbe non esserci alcuno spazio di manovra per chi volesse impugnare il provvedimento di sequestro, in quanto, la restituzione degli atti consentirebbe il pieno riespandersi del diritto di proprietà sul bene, comportando, come effetto, quello di far venir meno qualsiasi interesse all'impugnazione del provvedimento.

Tuttavia, soprattutto quando oggetto del sequestro sia l'intero *hard disk* di un *computer*, sorgono ulteriori profili di discussione. Il più importante riguarda la tutela del diritto alla riservatezza di colui che subisce lo spossessamento del bene. Infatti a seguito di copiatura dell'intero supporto informatico è messo a disposizione dell'autorità procedente un gran numero di informazioni personali non pertinenti al reato sulle quali il soggetto titolare potrebbe vantare un diritto alla distruzione. Il tema si presenta così in tutta la sua complessità: lo strumento del riesame, ove fosse ammesso anche rispetto a tale situazione, andrebbe non più a tutelare il diritto di proprietà leso dal provvedimento dell'autorità giudiziaria, ma il

diritto alla riservatezza del soggetto sottoposto alle indagini[68]. Su tale questione si è pronunciata la Corte di cassazione a Sezioni Unite in una rilevante pronuncia intervenuta a ridosso dell'entrata in vigore della l. n. 48/2008[69].

Il punto di partenza dell'argomentazione fatta propria dalle Sezioni Unite della Corte di cassazione è rappresentato dall'autonomia del provvedimento di copia del documento *ex* art. 258 c.p.p. rispetto a quello di sequestro. La predisposizione di un duplicato di quanto sequestrato, infatti, deriva da condizioni e ha alla base motivazioni autonome rispetto a quelle del provvedimento ablativo. L'atto di acquisizione tramite copia dei documenti risulta autonomo e distinto rispetto a quello di sequestro. Alla luce del principio di tassatività delle impugnazioni, in assenza di una espressa previsione, deve ritenersi, secondo la Suprema corte non espandibile il riesame avverso tale ultimo provvedimento.

Nella discussione *de* qua, i magistrati del Supremo Collegio si sono preoccupati anche di sottoporre a serrata critica l'idea per cui attraverso la richiesta di riesame del provvedimento di sequestro l'indagato o imputato, miri, in realtà, ad evitare che il documento duplicato entri a far parte del compendio probatorio[70]. Secondo questa impostazione l'illegittimità del sequestro farebbe cadere, sulla base della teoria dei frutti dell'albero avvelenato, anche l'atto di acquisizione tramite copia dei documenti. Questo sarebbe il vero risultato cui aspirerebbe l'impugnante. Tuttavia, sottolinea la Cassazione, questo orientamento finisce per di-

[68] Cfr. S. CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare* in *Dir. pen. proc.*, 2008, p. 479.

[69] Ci si riferisce a Cass. sez. Un., 24 aprile 2008, Tchmil, in *C.e.d. cass.* n. 239397 nonché in *Cass. pen.*, 2008, pp. 4031 ss. con osservazioni di E. APRILE.

[70] Secondo una parte della giurisprudenza, lo strumento del riesame del decreto di sequestro probatorio avrebbe una duplice funzione: non solo tutelare colui il quale abbia subìto lo spossessamento del bene, ma anche permettere alla persona sottoposta alle indagini o all'imputato di poter ottenere una pronuncia che vada ad eliminare dal compendio probatorio l'elemento sequestrato in maniera illegittima. Cfr. Cass. sez. IV, 1° dicembre 2005, Galletti, in *C.e.d. cass.* n. 233402.

latare eccessivamente la nozione di interesse ad impugnare. Quest'ultimo, secondo l'orientamento tradizionale, deve essere, infatti, concreto ed effettivo: l'impugnazione deve mirare, in altri termini, a rimuovere un provvedimento illegittimo lesivo di un diritto del singolo. Nel caso di cui si discute, mancherebbe proprio tale requisito di concretezza, in quanto la possibilità che il materiale acquisito sia poi effettivamente utilizzato è solamente eventuale. Alto sarebbe il rischio di ammettere un rimedio processuale finalizzato all'astratta osservanza della legge, privo di un effettivo risultato favorevole per l'impugnante. Non solo. Ad essere problematico sarebbe anche il rapporto che, secondo l'impostazione in oggetto, si instaurerebbe tra il procedimento incidentale e quello principale.

Di norma i due viaggiano, come è noto, su binari paralleli, senza che l'uno interferisca con l'altro[71]. Da questo punto di vista, il procedimento di riesame non fa eccezione: la restituzione della cosa sottoposta a sequestro non pregiudicherebbe l'utilizzabilità o meno di quanto acquisito tramite copia[72].

Dal canto suo la dottrina ha criticato l'impostazione accolta dai giudici di legittimità proprio a causa della particolarità del dato informatico. Infatti, come precisato precedentemente, all'interno dei sistemi informatici può essere contenuto un gran numero di informazioni rilevanti[73]. In questo contesto, la disciplina che prevede la restituzione del supporto all'interessato, ma che lascia nelle disponibilità dell'autorità giudiziaria le copie non appare idonea a tutelare il diritto del singolo ad evitare che dati di carattere privato siano detenuti

[71] Cfr. le considerazioni di Corte cost., 24 aprile 2009, n. 121, in *Giur. cost.*, 2009, pp. 1131 ss., la quale ha sancito l'incostituzionalità dell'art. 405, co. 1 *bis* c.p.p., il quale imponeva al pubblico ministero, al termine delle indagini preliminari, di richiedere l'archiviazione della notizia di reato tutte le volte in cui la Corte di cassazione si fosse pronunciata sull'insussistenza dei gravi indizi di colpevolezza di cui all'art. 273 c.p.p.

[72] Dal canto suo, rileva S. CARNEVALE, *op. cit.*, p. 478 come, da un punto di vista meramente pratico, un provvedimento che ordina la restituzione del materiale trattenuto in copia avrebbe rilevanti conseguenze sul procedimento principale in quanto gli inquirenti sarebbero materialmente impediti nell'utilizzazione di un documento non più in loro possesso.

[73] V. Cap. II, § 1.

dagli inquirenti senza che questi siano pertinenti per l'accertamento di un fatto di reato ovvero a prescindere dal fatto che siano stati ottenuti legittimamente o no[74]. Lo strumento del riesame del sequestro probatorio potrebbe così essere utilizzato per finalità nuove: evitare che siano trattenute dall'autorità procedenti informazioni di carattere personale che non hanno alcuna attinenza per le indagini preliminari o che siano stati acquisiti illegittimamente. In tal senso, prosegue la dottrina, proprio le indicazioni fornite dalla più volte citata l. n. 48/2008 dovrebbero essere opportunamente valorizzate. La novella, infatti, muove dall'idea del *computer* come mero contenitore accidentale del dato informatico che va da questo estratto con le opportune tecniche di *computer forensics*. Proprio questo richiamo alle metodologie più idonee per la copiatura del dato, unito alla considerazione dei rilevanti interessi che potrebbero venir lesi da una semplice copiatura integrale del supporto informatico, valgono a ritenere l'attività di copiatura dell'*hard disk* non come mera attività di conservazione di tracce ma come sequestro di materiale conoscitivo[75]. In tale ottica, l'interesse ad ottenere la restituzione della copia non sarebbe astratto, in quanto il riesame punterebbe a tutelare una ben più concreta posizione giuridica del singolo.

Più di recente il tema è tornato alla ribalta grazie ad un'interessante pronuncia delle Corte di cassazione[76]. Anche in questo caso, la controversia nasceva dal sequestro di dati informatici di proprietà di un giornalista. La decisione *de qua* riprende parte delle motivazioni fatte proprie dalle Sezioni Unite in tema di interesse ad impugnare il decreto di sequestro di un *hard disk* allorché questo sia già stato restituito. Ciò nonostante, vengono effettuate delle

[74] In tal senso si esprime, S. CARNEVALE, *op. cit.*, p. 479.

[75] Cfr., S. CARNEVALE, *op. cit.*, p. 481.

[76] Si fa riferimento a Cass. sez. VI, 24 febbraio 2015, Rizzo, in *C.e.d. cass.* n. 264092. Più recentemente, l'indirizzo citato è stato fatto proprio anche da Cass. sez. III, 23 giugno 2015, Cellino, in *C.e.d. cass.* n. 265181.

interessanti precisazioni in tema di interesse all'impugnazione allorché oggetto del sequestro siano dei dati informatici riservati.

La Corte, sulla base di una lettura degli istituti modificati dalla più volte citata l. n. 48/2008, rileva come oggetto del sequestro siano i dati informatici in quanto tali e non il supporto su cui questi sono contenuti. In questo senso, sottolinea come il concetto di copia e duplicazione degli stessi assuma, proprio in ragione delle proprietà intrinseche dei dati informatici, un particolare significato[77]. Alla luce di tale premessa, l'acquisizione mediante copia *ex* art. 258 c.p.p. e la restituzione del dispositivo elettronico non possono essere equiparati ad un dissequestro tutte le volte in cui il soggetto sia privato del valore del dato trattenuto. I casi cui fanno riferimento i giudici sono quelli in cui l'informazione acquisita si caratterizzi per la sua riservatezza. Rispetto a tale situazione la mera riconsegna del supporto non esaurisce la questione attinente alla restituzione dell'oggetto di sequestro. Questo ha, nella maggior parte dei casi, un valore minimo, soprattutto se confrontato con quello delle informazioni che vi sono contenute. In questa prospettiva si può parlare di dissequestro soltanto allorché venga reintegrata la perdita subita dal titolare del bene a causa del provvedimento di sequestro. Va detto, però, che, secondo la Suprema corte, il concetto di perdita va parametrato sulla base del diritto sostanziale leso dal provvedimento, per cui in tale nozione non rientra l'interesse a che una determinata cosa sia esclusa dal compendio probatorio[78].

[77] V. Cap. II, § 1.

[78] Nel caso concreto il ricorso è stato rigettato a causa dell'indeterminatezza dello stesso, il quale non specificava quali informazioni fossero state apprese, rendendo impossibile l'operazione di riconduzione del materiale sequestrato all'area tutelata dall'art. 203 c.p.p.

3. L'acquisizione dei dati di carattere informatico

Dopo aver esposto le problematiche afferenti alle perquisizioni, ispezioni e sequestri di materiale informatico, occorre porre attenzione ad un tema centrale per quanto riguarda la raccolta di prove digitali "statiche": quello avente ad oggetto le modalità di acquisizione di tali elementi.

Sul punto si registra un vivace dibattito, che da un lato vede contrapposte la giurisprudenza alla dottrina e che dall'altro registra un ampio spettro di opinioni. Gli istituti processuali che vengono richiamati nella discussione sono quelli dei rilievi compiuti dalla polizia giudiziaria *ex* art. 354 c.p.p. e degli accertamenti, tanto ripetibili quanto irripetibili, disposti dal pubblico ministero a norma degli artt. 359 e 360 c.p.p. Al fine di una compiuta trattazione della materia, prima di dar conto delle diverse opinioni dottrinali e giurisprudenziali in tema di acquisizione di elementi di natura informatica, è opportuno effettuare una, pur sintetica, ricognizione degli istituti citati.

L'art. 354 c.p.p. disciplina la complessa tematica degli accertamenti urgenti che può compiere la polizia giudiziaria sulla scena del crimine[79]. Il compito principale affidato alla stessa è quello di conservare, almeno fino al momento in cui il pubblico ministero non possa intervenire, le tracce del reato. In questa cornice il legislatore ammette che la polizia giudiziaria, allorché vi sia il pericolo di distruzione o dispersione di elementi probatori ritrovati sulla scena del crimine, possa disporre gli opportuni accertamenti e rilievi. Questi vengono descritti dalla dottrina come tutte quelle attività di osservazione, apprensione di cose, tracce

[79] Più in generale, in relazione all'attività della polizia giudiziaria nelle indagini preliminari si rimanda a F. CASSIBBA, *Investigazioni ed indagini preliminari*, in *Dig. pen.*, Utet, Torino, 2004, agg. II, pp. 515 ss.; S. GIAMBRUNO, *Polizia giudiziaria,* in *Dig. pen.*, Utet, Torino, 1995, vol. IX, pp. 597 ss.; V. PISANI, *Atti della polizia giudiziaria*, in *Enc. giur. Treccani*, 2007, pp. 1 ss.

ed elementi del reato sottoposti al pericolo di un'immediata modificabilità di carattere irreversibile[80]. Nel compimento di tali atti la polizia giudiziaria può utilizzare, qualora sia necessario, gli opportuni strumenti di carattere tecnico-scientifico che si palesino idonei alla conservazione e descrizione della scena del crimine. Sul punto, bisogna precisare come il potere della polizia giudiziaria in materia non sia illimitato. Questa, infatti, è legittimata esclusivamente a compiere attività di carattere materiale che non comportino alcuna valutazione di carattere scientifico[81]. Queste attività vengono definite tecnicamente come rilievi e si distinguono dagli accertamenti tecnici di natura peritale che sono, invece, di competenza del pubblico ministero[82].

La disposizione in commento è stata tra quelle oggetto di interpolazione dalla l. n.48/2008, la quale ha espressamente previsto che l'attività di conservazione delle tracce del reato possa riguardare anche i dati informatici. Inoltre, è stata sancita la possibilità per gli operanti di polizia giudiziaria di poter effettuare copia delle informazioni contenute in un elaboratore elettronico, purché questa sia compiuta con modalità tali da assicurare la conformità tra copia ed originale. Come si avrà modo di chiarire più avanti, la modifica legislativa non è, tuttavia, in grado di offrire una soluzione a tutte le questioni attinenti alle modalità di acquisizione del dato informatico.

[80] Così, L. D'AMBROSIO – P. L. VIGNA, *La pratica di polizia giudiziaria*, Cedam, Padova, 6° ed., 2006, p. 225.

[81] V., in tal senso, F. DE LEO, *Le indagini tecniche di polizia. Un invito al legislatore*, in *Cass. pen.*, 1996, pp. 697 s.

[82] Non mancano, in dottrina, voci contrarie a tale distinzione. Secondo alcuni, infatti, gli accertamenti tecnici potrebbero essere fatti rientrare nel generale potere di conservazione delle tracce del reato che, *ex* art. 348, co. 1° e 4° c.p.p., spetta alla polizia giudiziaria. L'unico limite rinvenibile sarebbe ricavabile non dalla natura dell'atto che gli operanti intendono effettuare, ma dalle sue conseguenze. Nella specie, alla polizia giudiziaria sarebbe precluso il compimento di qualsiasi operazione che possa irrimediabilmente incidere sulle scelte investigative del pubblico ministero. Cfr., sul punto L. D'AMBROSIO – P. L. VIGNA, *op. cit.*, p. 231.

Diversa è la prospettiva che emerge dagli artt. 359, 360 c.p.p., i quali vanno a disciplinare l'attività dei consulenti tecnici durante la fase delle indagini preliminari[83]. La prima disposizione ammette un generale potere di nomina, da parte del pubblico ministero, di un consulente tecnico al fine di svolgere «accertamenti, rilievi segnaletici, descrittivi o fotografici» e qualsiasi altra operazione per lo svolgimento della quale sia necessario possedere specifiche competenze. Come rilevato dalla dottrina, le operazioni che può legittimamente compiere il consulente tecnico sono di carattere complesso. Queste possono essere raggruppate in tre categorie. In primo luogo, il consulente tecnico può essere chiamato al solo fine di raccogliere dati o informazioni dalla scena del crimine allorché sia necessario utilizzare particolari metodologie per il compimento di tale attività, in secondo luogo, può essere richiesta la sua partecipazione in sede di elaborazione critica di quanto da altri repertato, in terzo luogo, il consulente tecnico può trovarsi nella situazione di dover svolgere entrambe le operazioni appena descritte[84].

Nella scelta del soggetto cui affidare lo svolgimento delle operazioni, il pubblico ministero gode di una certa autonomia. Questi, infatti, non è obbligato a scegliere una persona che sia iscritta all'albo dei periti[85]. Eventuali questioni circa la validità e l'attendibilità dei risultati raggiunti possono essere oggetto di discussione in sede dibattimentale.

---

[83] Per ulteriori riferimenti bibliografici ed un inquadramento generale del tema, v., D. CURTOTTI NAPPI, – L. SARAVO, *Sopralluogo giudiziario*, in *Dig. pen.*, Utet, Torino, 2011, agg. VI, pp. 587 ss.; D. CURTOTTI, *Rilievi e accertamenti tecnici*, Cedam, Padova, 2013, pp. 1 ss.;F. GIUNCHEDI, *Accertamenti tecnici*, in *Dig. pen.*, Utet, Torino, 2010, agg. V, pp. 1 ss.; F. GIUNCHEDI, *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, Utet, Torino, 2009, pp. 23 ss.; P. NOCITA, *Consulente tecnico II) diritto processuale penale*, in *Enc. giur. Treccani*, 1988, pp. 1 ss.

[84] Cfr., M. COSSIGNANI, *Il contributo tecnico nel processo: la novità della consulenza* extra perita, in *Dir. pen. proc.*, 1997, p. 335, il quale applica alla consulenza tecnica in fase investigativa la tripartizione dei compiti del perito proposta da F. CORDERO, *op. cit.*, pp. 781 s. Per una panoramica più generale sulle tipologie di consulenze ammesse dal codice di rito penale, si rimanda a R. E. KOSTORIS, *op. cit.*, pp. 28 ss.

[85] In giurisprudenza, v. Cass. sez. III, 23 novembre 2005, Pellegri, in *C.e.d. cass.* n. 233192

La particolarità più importante che deve essere segnalata per quanto attiene agli accertamenti tecnici, riguarda la tutela del diritto di difesa dell'indagato. Al riguardo vale la pena ricordare come le operazioni tecniche ricomprese nell'art. 359 c.p.p. vengano compiute senza che sia dato alcun avviso al difensore del soggetto sottoposto alle indagini[86]. La motivazione di tale scelta è riconnessa alla natura degli accertamenti che possono essere effettuati, i quali si caratterizzano per la loro ripetibilità.

Dal canto suo, l'art. 360 c.p.p. disegna una modalità nettamente diversa di acquisizione di elementi probatori formati grazie al consulente tecnico. Il fulcro di tale disposizione è da ricercare nell'idea di garantire un contraddittorio anticipato nella fase delle indagini preliminari in relazione all'acquisizione dell'elemento di prova[87]. La disposizione *de qua*, infatti, prevede che, allorché l'accertamento tecnico debba vertere su persone, cose o luoghi soggetti a modificazione, il pubblico ministero sia tenuto ad avvisare la persona sottoposta alle indagini, la persona offesa e i loro difensori del giorno, dell'ora e del luogo di conferimento dell'incarico al consulente tecnico. Nella medesima comunicazione i soggetti citati devono essere informati della facoltà di nominare propri consulenti tecnici.

Il presupposto in grado di far scattare la procedura di cui all'art. 360 c.p.p. è quello della non ripetibilità dell'atto che deve essere compiuto. La disposizione non contiene una definizione precisa del concetto di irrepetibilità[88]. Cosicché appare necessario procedere per gradi, occorre osservare, anzitutto, come al comma 1°, l'art. 360 c.p.p. faccia riferimento ad

[86] Cfr. Cass. sez. VI, 14 ottobre 2008, Nirta, in *C.e.d. cass.* n. 242385; Cass. sez. I, 20 marzo 2013, Tellay, in *C.e.d. cass.* n. 256237.

[87] L'effettiva realizzazione di tale risultato è stata, almeno in parte, sottoposta a critica. Ciò in quanto, come rilevato da alcuni, il legislatore avrebbe creato un «contraddittorio imperfetto», in quanto l'organo che presiede alla corretta formazione della prova non è terzo, essendo questi il pubblico ministero. Sul punto, v. R.E. KOSTORIS, *op. cit.*, pp. 148 s.

[88] La scelta è stata fatta consapevolmente dal legislatore, il quale nella stessa relazione al progetto preliminare afferma come la distinzione tra atto ripetibile e atto non ripetibile sia da lasciarsi all'esperienza pratica. Cfr. *Rel. prog. prel. c.p.p.* in *Speciale documenti giustizia*, II, 1988, p. 199.

accertamenti che hanno per oggetto persone, cose o luoghi soggette a modificazione. Successivamente, al comma 4°, si prevede la possibilità per l'indagato di effettuare una riserva di incidente probatorio, la quale ha il potere di bloccare l'attività del pubblico ministero, a meno che non ci si trovi in situazioni di particolare urgenza. In questo quadro si inserisce l'art. 117 disp. att. c.p.p. che estende l'istituto dell'accertamento tecnico irripetibile anche a quelle eventualità in cui l'atto non sia urgente, ma, tuttavia, il compimento delle attività tecniche sia tale da rendere l'atto non più ripetibile.

Dal quadro tratteggiato sembra emergere un concetto di irrepetibilità sfaccettato, all'interno del quale è possibile distinguere diverse ipotesi in relazione al tipo di causa che sta alla base della situazione di indifferibilità[89].

Da un canto vi sono le cause di non ripetibilità estrinseche. A questa categoria sono ascrivibili tutti quei casi in cui l'operazione tecnica sia astrattamente ripetibile, ma in cui il passare del tempo possa rendere la stessa inutile. In questo senso la non ripetibilità deriva non da proprietà dell'oggetto analizzato, ma da fattori esterni allo stesso. Dall'altro canto vi sono le cause di non ripetibilità intrinseche, qui sono le modalità attraverso cui si svolge l'atto a rendere lo stesso non più ripetibile.

Volgendo lo sguardo alle modalità di acquisizione del dato informatico in sede di indagini preliminari, sembrerebbe che il legislatore abbia preso una posizione relativamente chiara. Infatti le modifiche intervenute con l. n. 48/2008 sembrano voler ricondurre tali operazioni alla fattispecie dei rilievi. Ciò emerge già dalla lettura dell'art. 354, co. 2° c.p.p. e dal

[89] Sul punto, si fa riferimento alla suddivisione proposta da R.E. KOSTORIS, *op. cit.*, pp. 155 s.

potere che questa disposizione assegna alla polizia giudiziaria di effettuare copia dei dati informatici ritrovati sulla scena del crimine[90].

Alcuni studiosi hanno salutato con favore la scelta legislativa di consentire già alla polizia giudiziaria di compiere le operazioni finalizzate all'acquisizione di dati informatici[91].Tale soluzione troverebbe, sistematicamente, riferimento nelle disposizioni generali in tema di indagini preliminari. Al riguardo, occorre ricordare come l'art. 348 c.p.p. – disciplinante l'attività di assicurazione delle fonti di prova da parte della polizia giudiziaria – faccia riferimento alla possibilità per la stessa di poter utilizzare «persone idonee» allorché sia necessario svolgere operazioni che richiedano specifiche competenze tecniche. Questi soggetti non sono dei consulenti tecnici, in quanto si occupano esclusivamente dello svolgimento di attività materiali. Sono definibili come persone dotate di particolari abilità operative[92].

A sua volta, il già citato art. 354, co. 2° c.p.p. impone agli organi di polizia una sorta di obbligazione di risultato, laddove precisa che i dati informatici devono essere raccolti usando misure tecniche idonee a salvaguardarne l'integrità.

La lettura combinata degli artt. 348, co. 4° e 354, co. 2° c.p.p. condurrebbe a ritenere che alla polizia giudiziaria, attraverso le sue sezioni specializzate si sia voluto consentire di intervenire sulla scena del crimine e di acquisire, senza alcuna partecipazione della difesa, dati informatici[93].

---

[90] Cfr. M. DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, p. 442, il quale, come si vedrà in seguito, critica l'opzione fatta propria dal legislatore.

[91] In tal senso F.M. MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, pp. 1264 s.

[92] Sulla distinzione tra le persone idonee di cui all'art. 348, co. 4° c.p.p. e i consulenti tecnici del pubblico ministero, v. R. E. KOSTORIS, *op. cit.*, p. 138.

[93] Ancora, F.M. MOLINARI, *op. cit.*, p. 1265.

Un altro filone dottrinale giunge alle medesime conclusioni seguendo un percorso argomentativo leggermente differente. Questa dottrina prende le mosse dalla già accennata distinzione tra rilievi ed accertamenti, riconducendo l'attività di copiatura tra i primi. Infatti la clonazione di un supporto informatico sarebbe da considerare come una mera repertazione di materiale presente sulla scena del crimine[94]. Le difficoltà di carattere tecnico collegate al compimento dell'operazione non varrebbero a mutarne la natura.

I sostenitori della tesi *de qua* ricordano, in proposito, come allorché sia necessario repertare delle impronte dattiloscopiche, i consulenti siano autorizzati a utilizzare i mezzi tecnici più idonei in relazione alla superficie su cui sono presenti le impronte; e come ciò nonostante, venga qualificata questa attività come mero rilievo. Il caso della di duplicazione di un *hard disk* non sarebbe troppo diverso: il consulente sarebbe chiamato a scegliere lo strumento di *computer forensics* più adatto allo scopo, ben sapendo che questa operazione potrebbe non essere più ripetibile[95].

Ricondotte le attività di acquisizione del dato digitale all'interno della categoria dei rilievi, diventa relativamente semplice escludere l'applicabilità della procedura di cui all'art. 360 c.p.p., riservata, *per tabulas*, agli accertamenti[96].

La giurisprudenza di legittimità non si discosta eccessivamente dall'orientamento citato, riconoscendo all'acquisizione di dati informatici il valore di mero rilievo ed, escludendo, di conseguenza, la possibilità di applicare la più garantita procedura di cui all'art. 360 c.p.p.

[94] S. FASOLIN, *La copia di dati informatici nel quadro delle categorie processuali* in *Dir. pen. proc.*, 2012, p. 376.

[95] S. FASOLIN, *op. cit.*, p. 377.

[96] È, infatti, la stessa dizione letterale dell'art. 360 c.p.p. ad escludere che la procedura ivi descritta possa essere utilizzata anche per il compimento di rilievi, ancorché particolarmente complessi. Come rilevato da R. E. KOSTORIS, *op. cit.*, p. 150, il mancato inserimento del termine rilievi della disposizione citata non è frutto di una svista del legislatore, il quale ha deciso di eliminare il riferimento ai rilievi nel passaggio dal testo del progetto preliminare a quello definitivo.

alla fattispecie in commento[97]. Il punto di partenza dell'argomentazione della Corte è rappresentato dalla ricostruzione del concetto di non ripetibilità dell'atto. Questo, nel suo nucleo fondamentale, è delineato in relazione al dibattimento: l'atto investigativo può qualificarsi come irripetibile tutte le volte in cui la sua ripetizione nella fase del giudizio risulti impossibile oppure inidonea ad ottenere i medesimi elementi probatori. Successivamente, viene ribadita la differenza tra rilievi e accertamenti tecnici: mentre i primi si caratterizzano per essere operazioni di carattere materiale, i secondi comprendono un'attività di valutazione degli elementi raccolti. Così ricostruiti gli istituti, l'indirizzo riferito esclude che l'attività di copiatura debba essere svolta in base alla disciplina degli accertamenti tecnici irripetibili facendo riferimento ad una duplice argomentazione: tale operazione, infatti, non solo sarebbe di carattere meramente materiale e priva, pertanto, di quegli aspetti valutativi che varrebbero a ricondurla alla disciplina di cui all'art. 360 c.p.p.; ma, inoltre, non comporterebbe alcuna modificazione irreversibile dello stato delle cose, essendo sempre possibile riprodurre informazioni identiche a quelle contenute sul supporto originale[98].

Va detto, però, come esista in dottrina anche un orientamento che, appoggiandosi alla conclusione a cui giunge la giurisprudenza, sostiene l'applicabilità della disciplina degli accertamenti tecnici irripetibili alla copiatura del supporto informatico. All'interno di questo filone si distinguono, poi, diverse voci. Una prima linea argomentativa prende le mosse dalle caratteristiche del dato digitale, il quale, come chiarito in precedenza, è per sua natura fragile

[97] Si fa riferimento a Cass. sez. I, 2 aprile 2009, A.S.A., in *Dir. pen. proc.*, 2010, pp. 337 s. Più recentemente si sono inserite nel medesimo filone giurisprudenziale, tra le altre, Cass. sez. II, 19 febbraio 2015, Apicella ed altri, in *C.e.d. cass.* n. 263797; Cass. sez. II, 4 giugno 2015, Scanu ed altri, in *C.e.d. cass.* n. 264286.

[98] A parere di M. DANIELE, *op. cit.*, p. 443, le motivazioni sottese a tale orientamento sono tendenzialmente legate al timore che la libera disponibilità del *computer* da cui estrarre le informazioni nelle more dello svolgimento dell'accertamento tecnico irripetibile metterebbe in pericolo la fruttuosità dell'atto stesso. Infatti, alto sarebbe il pericolo che l'imputato possa decidere di cancellare o di danneggiare in maniera irreversibile i dati informatici rilevanti.

e volatile[99]. Ciò induce a ritenere che alte siano le probabilità che, attraverso un'attività non corretta, si verifichino fenomeni irreversibili di corruzione del dato informatico. Inoltre viene rilevato come la procedura stessa di copiatura possa comportare una modificazione delle informazioni raccolte. In questo senso, l'attività di duplicazione del supporto sarebbe riconducibile alla fattispecie delineata dall'art. 117 dist. att. c.p.p.[100].

Proprio l'intrinseca modificabilità del dato spingerebbe, comunque, verso una valorizzazione massima del contraddittorio: tramite la procedura di cui all'art. 360 c.p.p. i consulenti tecnici del pubblico ministero e della difesa potrebbero concordare, sulla base della situazione di fatto, le metodologie da applicare[101]. In questa maniera, non solo si garantirebbe la genuinità dell'elemento probatorio, ma, inoltre, si tutelerebbe il diritto di difesa dell'indagato.

Ad una soluzione non troppo dissimile giunge chi sottolinea come il fulcro della questione riguardante le modalità di duplicazione delle fonti di prova digitale sia da ricercare nella rielaborazione del concetto stesso di irripetibilità[102]. Sicuramente l'atto di *computer forensics*, come la maggior parte delle operazioni investigative, si caratterizza per la sua indifferibilità: il trascorrere del tempo potrebbe portare ad una modificazione dei dati informatici da acquisire. Inoltre, le modalità stesse di copiatura del supporto prescelte dall'operatore, modificando lo stesso in maniera irreversibile, potrebbero in alcuni casi rendere l'atto non reiterabile. Diventerebbe, quindi, di fondamentale importanza la verifica concreta circa l'invasività delle operazioni compiute in relazione alla genuinità del dato informatico raccolto.

[99] V., A. E. Ricci, Digital evidence *e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc.*, 2010, p. 344.

[100] Cfr. M. Daniele, *op. cit.*, p. 442.

[101] Ancora, A. E. Ricci, *op. cit.*, p. 345; F. Giunchedi, *Le* malpractices, cit., p. 829.

[102] Ci si riferisce ad E. Lorenzetto, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, pp. 1530 s.

Allorché le operazioni svolte siano state compiute in adesione alle migliori pratiche del settore, allora l'atto può «ben inserirsi tra quelli «indifferibili» suscettivi di compimento unilaterale[103]». Viceversa, nel caso in cui l'attività di riproduzione dei dati ne abbia comportato una mutamento, l'utilizzazione processuale di quanto raccolto può dirsi legittima soltanto se preceduta dallo svolgimento dell'atto in contraddittorio tra le parti *ex* art. 360 c.p.p.[104].

In questo scenario compete al giudice la riconduzione dell'atto ad una delle due categorie citate – accertamenti tecnici ripetibili *ex* art. 359 c.p.p. o accertamenti tecnici irripetibili *ex* art. 360 c.p.p. – «attraverso la doverosa verifica *a posteriori* sul corretto operato del soggetto inquirente[105]».

[103] Così, E. LORENZETTO, *op. cit.*, p. 1530.

[104] Cfr. E LORENZETTO, *op. cit.*, p. 1531.

[105] Ancora, E. LORENZETTO, *op. cit.*, p. 1531. Parrebbe accettare una tale prospettiva anche V. ZAMPERINI, *op. cit.*, pp. 516 ss.

4. La conservazione dei dati relativi al traffico telematico per finalità afferenti alle indagini penali

Il tema dell'acquisizione dei dati relativi al traffico in possesso dei fornitori di connettività è stato al centro di numerose discussioni e, al contempo, oggetto ripetuto di interventi legislativi[106]. Al riguardo è necessario, prima di entrare *in medias res*, effettuare una prima premessa. Dato l'oggetto del presente lavoro, il tema della conservazione dei dati citati non potrà che essere affrontato esclusivamente in riferimento ai dati di carattere telematico, ben consapevoli che in questo modo rimane fuori dall'area di indagine la complessa questione riguardante i tabulati telefonici[107].

Da un punto di vista cronologico il primo riferimento alla possibilità per l'autorità giudiziaria di ottenere copia dei dati di traffico risale ai primi anni 2000, allorché il legislatore ha dato attuazione alla direttiva 2002/58/CE[108]. Il d.lgs. 30 giugno 2003, n. 196, rubricato codice in materia di protezione dei dati personali, disciplinava, all'art. 132, l'obbligo di conservazione dei «dati relativi al traffico telefonico» da parte dei fornitori dei medesimi servizi. Tale disposizione venne successivamente modificata dal d.l. 24 dicembre 2003, n. 353, il quale, tra le altre cose, eliminò il termine «telefonico» dal citato art. 132, ammettendo una definizione

[106] Per una più ampia panoramica di carattere storico sugli interventi legislativi che si sono succeduti sul tema, si rimanda a A. STRACUZZI, Data retention*: il faticoso percorso dell'art. 132 codice* privacy *nella disciplina della conservazione dei dati di traffico* in *Dir. inf.*, 2008, pp. 585 ss.

[107] Per un quadro generale sulla tematica dei dati di carattere personale registrati ai fini della repressione penale, v. S. SIGNORATO, *Il trattamento dei dati personali per fini di prevenzione e repressione penale*, in *Riv. dir. proc.*, 2015, pp. 1484 ss.

[108] Prima che fosse emanata la disciplina in commento, per ottenere i dati esterni delle comunicazioni si ricorreva allo strumento previsto dall'art. 256 c.p.p. Sul punto, si erano espresse le stesse Sezioni Unite della Corte di cassazione attraverso la sentenza Cass. sez. Un., 23 febbraio 2000, D'Amuri, in *C.e.d. cass.* n. 215841. Per una ricostruzione del dibattito sul punto, v. C. CONTI, *L'attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, in *Le nuove norme sulla sicurezza pubblica*, a cura di S. Lorusso, Cedam, Padova, 2008, pp. 4 ss.

di dati di traffico così ampia da poter ricondurre nella stessa anche i dati di carattere telematico. Tuttavia, in sede di conversione del citato decreto legge l'art. 132 Codice *privacy* venne totalmente riscritto ripristinando il riferimento ai «dati relativi al traffico telefonico» e, rendendo quindi, inoperante l'obbligo di trattenimento ai dati di carattere telematico. Soltanto il successivo intervento del legislatore, ad opera del d.l. 27 luglio 2005, n. 144 conv. in l. 31 luglio 2005, n. 155, reintrodusse il riferimento ai dati relativi al traffico anche telematico. La successiva tappa della travagliata storia legislativa dell'art. 132 Codice *privacy* si è avuta nel 2008, allorché il legislatore è intervenuto due volte: tramite la l. n. 48/2008 e il d.lgs. 30 maggio 2008, n. 108. Quest'ultimo provvedimento è stato emanato al fine di recepire la direttiva 2006/24/CE[109].

Come rilevato dalla dottrina, la complessa evoluzione della normativa *de qua* è emblematica della delicatezza del problema ad essa sotteso. Infatti, il trattenimento dei dati relativi al traffico pone delicati problemi di bilanciamento tra le esigenze di riservatezza del singolo e quelle di sicurezza della collettività[110].

Dal punto di vista tecnico, i dati che vengono conservati e richiesti dall'autorità giudiziaria sono, da un lato, quelli rilevanti per l'identificazione di un soggetto che opera nella rete *Internet* e, dall'altro, quelli riguardanti l'attività di navigazione dello stesso – c.d. *file* di *log*[111]. Più precisamente, allorché taluno si connetta alla rete *Internet*, l'I.S.P. gli assegna un

[109] Sul punto, v. Cap. III § 2.

[110] La tematica assume maggior spessore alla luce dell'importanza che i dati sul traffico possono ricoprire nelle indagini riguardanti i fenomeni di terrorismo, v. in tal senso S. SIGNORATO, *Contrasto al terrorismo e* data retention*: molte ombre e poche luci*, in *Il nuovo 'pacchetto' antiterrorismo*, a cura di R. E. Kostoris – F. Viganò, Giappichelli, Torino, 2015, p. 77. Per uno sguardo d'insieme sulle operazioni di sorveglianza di massa compiute attraverso la registrazione e l'analisi dei dati di traffico telematico e non solo negli Stati Uniti d'America, si rimanda a V. FANCHIOTTI, *Il cyberorecchio di Dionisio*, in *Cass. pen.*, 2015, pp. 1646 ss.

[111] Cfr. G. VACIAGO, *La disciplina normativa sulla* data retention *e il ruolo degli* Internet Service Provider, in Internet Provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, a cura di L. Lupária, Giuffrè, Milano, 2012, p. 141.

indirizzo I.P., il quale identifica il soggetto nell'arco di tutta la sua attività di navigazione[112]. L'autorità giudiziaria può, come si vedrà meglio più avanti, chiedere al fornitore di connettività i dati afferenti ad un determinato indirizzo I.P. in modo da identificare il soggetto che si è connesso[113]. Viceversa, i *file* di *log* sono quei *file* in cui sono memorizzate tutte le attività compiute da un determinato utente per tutta la durata della sua connessione.

Se quelle descritte sono le due principali categorie di dati richieste dall'autorità giudiziaria, deve essere rilevato come, dal canto suo, il legislatore non sembrerebbe aver effettuato una compiuta delimitazione della tipologia di informazioni che possono essere crichieste ai fornitori di connettività[114]. Infatti l'art. 4, co. 2° lett. *h*) Codice *privacy*, definendo i «dati di traffico» come «qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione», non sarebbe in grado di evidenziare i necessari confini tra dati relativi al traffico telefonico e dati relativi al traffico telematico. L'opportunità di una precisione maggiore nella definizione dei dati da conservare, la si coglie alla luce del disposto dell'art. 132, co. 1° Codice *privacy*, lad-

[112] Con il termine I.S.P. si fa riferimento agli *Internet Service Provider*, ossia a quelle società che si occupano di fornire ad un certo soggetto i servizi necessari per connettersi alla rete *Internet*. L'indirizzo I.P., invece, è costituito da una serie di numeri che sono in grado di identificare in maniera esclusiva un determinato *device* connesso alla rete *Internet*. Senza pretesa di esaustività, va sottolineato come esistano due tipologie di indirizzi I.P., quelli statici e quelli dinamici. I primi sono, di norma, assegnati ai *server* e sono stabili, per cui la sequenza numerica farà riferimento sempre alla stessa macchina. Viceversa, gli I.P. dinamici vengono assegnati ad ogni singola connessione e riassegnati allorché il soggetto si disconnette.

[113] Dato che, come sopra precisato, un singolo indirizzo I.P. è in grado di identificare una determinata macchina connessa alla rete, conoscendo l'ora precisa di connessione è possibile risalire al *device* utilizzato per la navigazione. Tuttavia, come rilevato, tra gli altri da G. VACIAGO, *op. cit.*, pp. 156 s., questo tipo di accertamento non esaurisce l'attività investigativa, in quanto esistono numerose tecniche idonee a mascherare la propria identità sulla rete.

[114] Cfr. in tal senso, F. CERQUA, *Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche*, in *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 marzo 2008, n. 48)*, a cura di L. Lupária, Giuffrè, Milano, 2008, pp. 232 s.

dove si prevedeno tempi di conservazione diversi in relazione alla tipologia del dato. Ventiquattro mesi dalla data della comunicazione per quelli relativi al traffico telefonico, dodici mesi dalla data della comunicazione per quelli riguardanti il traffico telematico.

Tuttavia una soluzione a tale inconveniente può derivare dalla lettura dell'art. 3 d. lgs. n. 109/2008, il quale, viceversa, fornisce una esaustiva elencazione della tipologia di dati afferenti al concetto di traffico telematico. Da un punto di vista generale, si possono individuare cinque diverse categorie di dati che devono essere conservati e che possono essere acquisiti dall'autorità giudiziaria: quelli per rintracciare la fonte di una comunicazione; quelli per individuare la destinazione di una comunicazione; quelli per determinare la data, l'ora e la durata di una comunicazione; quelli, infine, per individuare gli strumenti di comunicazione utilizzati[115]. In considerazione dei rilevanti interessi che la normativa punta a proteggere, parte della dottrina ritiene il catalogo di cui all'art. 3 d. lgs. n. 109/2008 di carattere tassativo[116]. Tale considerazione comporta una rilevante conseguenza: non possono far parte dell'insieme dei dati conservati quelli riguardanti l'attività di navigazione del singolo utente. La cronologia dei siti *web* visitati non costituisce un dato esterno alla comunicazione, ma, più correttamente, fa parte del contenuto della stessa[117].

Per quanto attiene ai soggetti sottoposti all'obbligo di conservazione dei dati, merita di essere citata una delibera del Garante della protezione dei dati personali, il quale li individua come coloro «che realizzano esclusivamente o prevalentemente una trasmissione di

[115] Cfr. C. CONTI, *op. cit.*, p. 15.

[116] In tal senso, C. CONTI, *op. cit.*, p. 15.

[117] Si esprime a favore di tale opinione lo stesso Garante per la protezione dei dati personali nel parere *il Garante ai gestori Tlc: cancellate le informazioni sulla navigazione in Internet*, in *www.garanteprivacy.it*, docweb n. 1481285.

segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete e che offrono servizi a utenti finali secondo il principio di non discriminazione[118]».

Inoltre l'art. 132 Codice *privacy* individua tanto le finalità di conservazione dei dati, quanto i soggetti che possono ottenere copia di tali informazioni. Sul primo versante, si stabilisce *per tabulas* che l'obbligo di custodia dei dati ha esclusivamente finalità di repressione e accertamento dei reati. Come chiarito dalla dottrina, tale indicazione è da intendersi in senso tassativo: qualsiasi richiesta giunta ai fornitori di connettività con motivazioni diverse da quelle citate è da ritenersi illegittima.

Sul secondo versante, viene definita la platea dei soggetti processuali che possono richiedere copia dei dati conservati. Questi sono individuati non soltanto nel pubblico ministero, ma anche nel difensore della persona sottoposta alle indagini e in quello della persona offesa dal reato. Come sottolineato da alcuni studiosi, la previsione merita di essere apprezzata per non aver ristretto esclusivamente all'organo dell'accusa il potere di ottenimento dei dati. Infatti questi ultimi possono rappresentare un sicuro approdo per l'elaborazione di un alibi convincente per l'imputato[119].

Da ultimo l'art. 132 Codice *privacy*, in ragione dei rilevanti interessi toccati dalla disposizione, affronta il tema della protezione dei dati conservati. Infatti si impone che il Garante per la protezione dei dati personali individui, attraverso un proprio provvedimento, le misure tecniche idonee ad evitare che la conservazione di tali informazioni si risolva in un

[118] Cfr. Garante per la protezione dei dati personali, *Misure e accorgimenti a garanzia degli interessati in tema di conservazione di dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati*, in *www.garanteprivacy.it*, docweb n. 1442463.

[119] V. in tal senso, S. SIGNORATO, *Contrasto*, cit., p. 76, nt 4.

vulnus per la riservatezza degli utenti[120]. Terminato il periodo di conservazione, i gestori di connettività sono tenuti a cancellare integralmente tutti i dati raccolti, eliminando, ovviamente, anche eventuali copie di *backup* degli stessi.

Oltre a quanto già illustrato, l'art. 132 Codice *privacy* ai commi 4 *ter*, 4 *quater* e 4 *quinquies* prevede la possibilità per l'autorità pubblica di ordinare ai fornitori e agli operatori di servizi informatici o telematici la conservazione dei dati relativi al traffico telematico, il c.d. *freezing*. Si tratta di una ulteriore e diversa fattispecie che autorizza il trattenimento dei dati esterni alla comunicazione. La differenziazione tra le due eventualità è di carattere principalmente temporale. L'effetto principale dell'ordine di cui all'art. 132, co. 4 *ter* Codice *privacy* è, infatti, quello di imporre il trattenimento dei dati per un periodo di novanta giorni. Questo termine si va a sommare a quelli di dodici mesi a partire dalla comunicazione previsto in via generale dall'art. 132, co. 1° Codice *privacy*. Si viene a configurare, di fatto, una sorte di potere di prorogare la conservazione dei dati relativi al traffico telematico[121].

Il numero dei soggetti legittimati all'emanazione del provvedimento in discorso appare relativamente ampio. Vi sono inclusi il Ministro dell'Interno, 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. Inoltre, grazie al richiamo all'art. 226 disp. att. c.p.p. in tema di intercettazioni preventive, sono legittimati ad ordinare il congelamento dei dati di traffico telematico, su delega del Ministro dell'Interno, anche i responsabili dei

[120] Per alcune esemplificazioni delle misure di sicurezza da attivare, v. C. CONTI, *op. cit.*, p. 21. Inoltre, G. VACIAGO, *op. cit.*, p. 149, stigmatizza l'idea per cui la predisposizione di tutte le misure di sicurezza sia esclusivamente a carico del fornitore del servizio, comportando un notevole onere economico a carico dello stesso.

[121] Si esprime in tal senso, C. CONTI, *op. cit.*, p. 24.

servizi specializzati centrali e interforze[122]; il questore; i comandanti provinciali dei Carabinieri e della Guardia di Finanza. Sul punto, la dottrina ha criticato la scelta legislativa compiuta in ragione dell'estrema varietà dei soggetti così individuati[123].

Altro aspetto che va a differenziare l'attività di congelamento dei dati telematici rispetto a quella di conservazione, è quello dei soggetti destinatari dell'obbligo. Infatti mentre l'art. 132, co. 1° Codice *privacy* fa riferimento soltanto ai fornitori di connettività, l'art. 132, co. 4 *ter* Codice *privacy*, viceversa, fa riferimento «ai fornitori e agli operatori di servizi informatici o telematici». La differenza non è marginale, in quanto, con l'espressione operatori di servizi informatici si intendono anche i c.d. *content provider*, ossia quelle società che forniscono contenuti per siti *Internet*[124]. L'effetto sembrerebbe essere quello di ampliare il novero dei dati acquisibili dall'autorità di pubblica sicurezza.

Da un diverso punto di vista, è stata sottoposta a critica la modalità di individuazione dei reati che possono giustificare il provvedimento in discorso. Infatti al di là del richiamo all'art. 226 disp. att. c.p.p., la disposizione fa riferimento alla «finalità di accertamento e repressione di specifici reati» senza, però, contenere alcun criterio per l'individuazione degli stessi. Così operando, il legislatore sembra aver creato un catalogo vuoto che potrebbe permettere l'acquisizione dei dati relativi al traffico telematico per qualsiasi illecito penale.

Anche il procedimento di acquisizione non risulta impermeabile ad alcune osservazioni critiche. Si prevede, infatti, che il fornitore di servizi debba ottemperare senza ritardo

[122] Si fa riferimento ai servizi specializzati centrali previsti dal d.l. 13 maggio 1991, n. 152 conv. con modificazioni nella l. 12 luglio 1991, n. 203. Più precisamente questi sono rappresentati dal Servizio Centrale Operativo e dai centri interprovinciali criminalpol per quanto attiene alla Polizia di Stato; presso l'Arma dei Carabinieri sono stati istituiti il Raggruppamento Operativo Speciale e le sezioni anticrimine; dal canto suo, la Guardia di Finanza ha creato il Servizio Centrale di Investigazione sulla Criminalità Organizzata e i Gruppi Interprovinciali di Investigazione sulla Criminalità Organizzata.

[123] Cfr. L. LUPÁRIA, *La ratifica*, cit., p. 722.

[124] Cfr. C. CONTI, *op. cit.*, pp. 24 s.; F. CERQUA, *op. cit.*, pp. 236 s.

ed assicurare immediatamente l'autorità procedente circa l'adempimento dell'ordine. Tale provvedimento deve, inoltre, essere comunicato al pubblico ministero del luogo di esecuzione, il quale può esercitare sullo stesso un potere di convalida. Tuttavia questa previsione rischia di risultare, in molti casi, lettera morta. La mancanza di una notizia di reato e, di conseguenza, di un pubblico ministero incaricato dello svolgimento delle indagini preliminari, rendono il controllo previsto dall'art. 132, co. 4 *quinquies* Codice *privacy* non effettivo[125].

Ulteriori questioni di carattere applicativo derivano dal difficile coordinamento della disciplina contenuta nell'art. 132 Codice *privacy* con quella di cui all'art. 256 *bis* c.p.p. Quest'ultima disposizione, introdotta dalla l. n. 48/2008, prevede che allorché l'autorità giudiziaria disponga il sequestro di dati detenuti dai fornitori di servizi informatici, questa possa imporre che l'acquisizione di tali informazioni avvenga attraverso la copia degli stessi con modalità tali da assicurarne la fedeltà agli originali[126]. Ad una prima lettura l'art. 256 *bis* c.p.p. sembrerebbe porsi in contraddizione con la complicata disciplina appena descritta: infatti, sembrerebbe affidare al pubblico ministero un generale potere di acquisizione di tutti i dati afferenti alle comunicazioni di carattere telematico[127].

Al fine di evitare un tale effetto la dottrina ha proposto una lettura di carattere sistematico che metta in relazione l'art. 256 c.p.p., disciplinante il sequestro di corrispondenza anche telematica, con la previsione in commento. In tale ottica, l'art. 256 *bis* c.p.p. andrebbe a disciplinare le modalità del sequestro di corrispondenza telematico, trovando la sua giustificazione in ragione della delicatezza dell'oggetto del sequestro. In altri termini, attraverso

[125] Si esprime sostanzialmente in tal senso, F. CERQUA, *op.cit.*, p. 238.

[126] L. LUPÁRIA, *La ratifica*, cit., p. 722 sottolinea come vi sia una sempre maggiore tendenza ad addossare a incombenti di carattere investigativo verso soggetti privati che potrebbero diventare concorrenti nel reato proprio a causa delle informazioni fornite all'autorità giudiziaria.

[127] Cfr. F. CERQUA, *op. cit.*, p. 239.

l'art. 256 *bis* c.p.p., il legislatore non avrebbe affidato un nuovo potere all'autorità giudiziaria, ma ne avrebbe disciplinato esclusivamente le modalità di esercizio[128].

Da ultimo, è necessario effettuare un richiamo all'art. 234 *bis* c.p.p. disposizione inserita dal legislatore attraverso il d.l. 18 febbraio 2015, n. 7 conv. in l. 17 aprile 2015, n. 43. L'articolo ammette la possibilità per l'autorità giudiziaria di acquisire documenti e dati informatici conservati all'estero sia nel caso in cui questi siano pubblici sia qualora questi siano «diversi da quelli disponibili al pubblico». Bisogna subito rilevare come ad un anno circa dall'entrata in vigore della norma, non sembra che questa sia stata oggetto di pronunce giurisprudenziali. La principale motivazione di tale evenienza potrebbe essere rintracciata nella difficoltà di comprensione e di inserimento nella sistematica del codice di rito penale di tale disposizione[129].

In primo luogo, vi è da chiarire l'àmbito oggettivo dell'art. 234 *bis* c.p.p., ossia a quali documenti e dati informatici questo faccia riferimento. Secondo alcuni studiosi l'insieme delle informazioni che possono essere acquisite grazie all'articolo in commento è molto ampio ed eterogeneo. Vi rientrerebbero, da un lato, tutte quelle informazioni liberamente reperibili sulla rete *Internet* (immagini, testi scritti, video, ecc.)[130]; dall'altro, potrebbero essere ricomprese nella previsione in discorso anche i c.d. metadati[131], anche se in quest'ultimo caso vi sarebbe da risolvere il delicato problema del rapporto tra il nuovo art. 234 *bis* c.p.p. e l'art.

[128] Si esprimono a favore di tale opzione interpretativa, F. CERQUA, *op. cit.*, pp. 239 s.; A. CISTERNA, *op. cit.*, p. 68; C. CONTI, *op. cit.*, p. 26.

[129] Nascono, inoltre, questioni riguardanti la disposizione in commento e le norme del codice di rito e non solo che disciplinano i rapporti con le autorità straniere. A parere di A. CISTERNA, *All'Aise l'attività d'informazione verso l'estero*, in *Guida dir.*, 2015, f. 19, p. 95, l'art. 234 *bis* c.p.p. non cambia le disposizioni riguardanti le rogatorie, essendo, comunque, necessario tale strumento per ottenere i documenti cui questo fa riferimento.

[130] Si esprime in tal senso, S. ATERNO, *L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nella* privacy, in *Arch. pen.*, 2016, n. 1, p. 165.

[131] Ancora, S. ATERNO, *op. cit.*, p. 166.

132 Codice *privacy* di cui si sono prima illustrate le problematicità. Secondo altri, l'espressione «dati informatici [...] anche diversi da quelli disponibili al pubblico» farebbe riferimento alla possibilità per l'autorità procedente di poter accedere anche a documenti e informazioni conservati nei sistemi di archiviazione *cloud* o in banche dati[132].

In secondo luogo, risulterebbe in parte oscuro il perimetro soggettivo della disposizione, in quanto questa contiene un troppo generico riferimento ai legittimi titolari dei dati da acquisire. L'espressione, infatti, sembrerebbe alludere alle persone titolari del potere di trattamento dei dati cui fa riferimento il Codice *privacy*[133]. Tuttavia, vi è chi sottolinea come tale espressione potrebbe coprire, in realtà, un àmbito soggettivo più ampio[134], tale da abbracciare tutti i soggetti titolari di diritti soggettivi nascenti dai contratti che i singoli utenti stipulano con le compagnie che forniscono servizi su *Internet*[135].

[132] V., L. VIOLA BERRUTI, Cyber terror*: esigenze di tutela preventiva e nuovi strumenti di contrasto*, in *www.lalegislazionepenale.eu*, pp. 3 s. Per alcune notazioni anche di carattere tecnico sull'acquisizione di materiale informatico conservato su sistemi *cloud*, v. C. FEDERICI, *Nuovi orizzonti per l'acquisizione remota di* Personal Cloud Storage, in *Questioni di informatica forense*, a cura di C. Maioli, Aracne, Roma, 2015, pp. 113 ss.

[133] Cfr. L. VIOLA BERRUTI, *op. cit.*, p. 3.

[134] Cfr. S. ATERNO, *op. cit.*, p. 168.

[135] Così, S. ATERNO, *op. cit.*, p. 168. I servizi cui si fa riferimento sono i più vari, sarebbero ricompresi in tale categoria non soltanto gli I.S.P., ma, più in generale, tutte le società che forniscono servizi agli utenti della rete.

5. Le intercettazioni di comunicazioni informatiche o telematiche

Come evidenziato precedentemente, allorché si faccia riferimento alle prove di carattere informatico costituenti un flusso di dati tra due terminali, la disposizione di riferimento è l'art. 266 *bis* c.p.p.[136]. Tuttavia, alla luce dell'eterogeneità delle modalità di presentazione di tale elemento probatorio, si discute tanto in dottrina quanto in giurisprudenza della possibilità di ricondurre nell'alveo del citato art. 266 *bis* tutta una serie di fattispecie diverse.

La prima questione da affrontare ha per oggetto il complesso tema delle modalità di acquisizione al processo penale sia dei messaggi inviati tra *smartphone* attraverso le varie piattaforme esistenti di *instant messanging* sia delle missive inviate tra *computer* attraverso lo strumento delle *e-mail*. Nonostante le differenze tecniche che sussistono tra i due mezzi di comunicazione, questi meritano di essere trattati assieme in quanto presentano, dal punto di vista del processo penale, forti analogie. Infatti, come si avrà modo di verificare nel prosieguo della trattazione, entrambi gli strumenti non solo costituiscono un sistema di comunicazione asincrono, in cui non c'è necessariamente contestualità nel dialogo[137], ma, inoltre, per il loro funzionamento necessitano di un *server* che si occupi di smistare i messaggi in entrata ed in uscita. Proprio quelli illustrati sono tra gli elementi che rendono maggiormente problematica la riconduzione di tali strumenti agli istituti del codice di rito penale.

La discussione ruota principalmente intorno ai confini tra l'istituto del sequestro di corrispondenza anche telematica di cui all'art. 254 c.p.p. e quello delle intercettazioni di comunicazioni informatiche cui fa riferimento l'art. 266 *bis* c.p.p.

[136] Per un generale inquadramento dell'istituto si rimanda alle considerazioni effettuate al Cap. II, § 3.

[137] Cfr. R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2008, p. 134.

Il dibattito si è sviluppato, in prima battuta, in relazione all'acquisizione delle *e-mail*. Da un punto di vista generale, l'art. 266 *bis* c.p.p., disciplinando una particolare modalità di intercettazione, parrebbe applicabile esclusivamente al caso in cui si abbia la possibilità di captare un messaggio *e-mail* mentre questo "viaggi" sulla rete telematica. Infatti la contestualità dello scambio comunicativo è tra gli elementi costitutivi del concetto stesso di intercettazione[138].

Tuttavia, una tale interpretazione è sembrata a taluno troppo restrittiva, restringendo l'applicabilità dell'art. 266 *bis* c.p.p. a casi relativamente marginali. Autorevole dottrina ha proposto una visione più ampia della fattispecie regolata dall'art. 266 *bis* c.p.p.[139]. Secondo questa ricostruzione il criterio di discrimine tra le intercettazioni e i sequestri delle missive elettroniche va ricercato nella conclusione o meno della comunicazione. Allorché l'*e-mail* sia inviata e letta dal destinatario, questa sarebbe da ricondurre, per analogia, alla lettera aperta e, come tale, sequestrabile dall'autorità giudiziaria attraverso la procedura di cui all'art. 254 c.p.p. Viceversa, allorché il messaggio non sia ancora stato aperto e, quindi, la comunicazione non sia andata a buon fine, si rientra ancora nell'àmbito applicativo dell'intercettazione di comunicazioni informatiche. Nelle situazioni di dubbio, ossia quando, nel momento in cui sorge l'esigenza di acquisire il dato non si possa essere sicuri circa la lettura o meno dell' *e-mail*, sarebbe preferibile scegliere sempre la procedura richiamata dall'art. 266 *bis* c.p.p. in quanto più rispettosa dei diritti coinvolti in tali atti[140].

---

[138] Cfr. E. M. MANCUSO, *L'acquisizione di contenuti* e-mail, in *Le indagini atipiche*, a cura di A. Scalfati, Giappichelli, Torino, 2014, p. 68.

[139] Si fa riferimento a quanto proposto da R. ORLANDI, *op. cit.*, pp. 134 s.

[140] Come notato sempre da R. ORLANDI, *op. cit.*, p. 135, il problema si pone principalmente allorché siano utilizzati servizi di *webmail*. In questo caso, l'*email client*, ossia l'applicativo utilizzato per leggere i messaggi, non è installato sul proprio *computer*, ma è costituito da un'applicazione *web* che svolge le proprie funzioni all'interno del *browser*. Al di là del tecnicismo, la differenza principale risiederebbe nel fatto che nel primo caso, lo "scaricamento" del messaggio può valere a far presumerne l'apertura. Nel secondo caso, quello dei servizi di *webmail*, non si avrebbe modo di sapere anticipatamente se i messaggi sono stati letti o meno dall'utente.

Seguendo una prospettiva completamente diversa, altri studiosi negano in radice la possibilità di ricondurre le attività di acquisizione dell'*e-mail* all'istituto delle intercettazioni di comunicazioni telematiche. L'argomentazione si fonda principalmente sulle differenze di carattere naturalistico tra l'operazione di intercettazione telefonica e l'apprensione di un messaggio di posta elettronica. Al riguardo, si rileva come, nel primo caso, l'autorità giudiziaria registri una comunicazione nel suo divenire. L'atto captativo è compiuto di pari passo con la formazione della conversazione[141]. Ciò giustifica il fatto che l'atto debba essere compiuto in regime di segretezza. Viceversa, nel caso dell'*e-mail* il contenuto comunicativo è formato e cristallizzato definitivamente in momento anteriore allo svolgimento dell'atto acquisitivo[142]. Tale situazione di fatto vale a non rendere necessaria la segretezza, essendo sufficiente, per la buona riuscita dell'atto, la sorpresa.

Nel medesimo senso si esprime quella dottrina che va, a sostegno della suddetta tesi, a sottolineare la portata innovativa delle modifiche apportate al codice di rito penale dalla più volte citata l. n. 48/2008. Questa è intervenuta, come è noto, riscrivendo non solo il 1° co. dell'art. 254 c.p.p., ma anche l'art. 353, co. 3° c.p.p. In entrambe le disposizioni, il legislatore ha inserito un esplicito richiamo alla corrispondenza inoltrata anche «anche per via telematica», comportando la riconduzione dell'*e-mail* sotto il concetto di corrispondenza[143]. La conseguenza di tale opzione interpretativa sarebbe l'applicabilità delle norme sul sequestro di corrispondenza anche all'*e-mail* e, quindi, della possibilità della polizia giudiziaria di poter

[141] V., M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 290.

[142] Cfr. M. DANIELE, *op. cit.*, pp. 290 s.

[143] Così, L. LUPÁRIA, *La ratifica,* cit., p. 722.

chiedere al gestore del servizio di posta elettronica di poter bloccare l'inoltro della corrispondenza di carattere telematico[144].

Un'ultima opzione interpretativa ha come punto di partenza la valorizzazione degli elementi di differenziazione tra i due atti investigativi[145]. Si sostiene che, infatti, mentre l'intercettazione avviene all'insaputa dei conversanti, il sequestro possa avvenire alla presenza dell'interessato. Se il primo atto è caratterizzato dalla segretezza, il secondo ha come elemento qualificante la sorpresa[146]. Partendo da tali considerazioni, l'indirizzo in esame sottolinea l'opportunità di distinguere a seconda della situazione concreta due principali eventualità. Da un canto, si pone il caso in cui l'autorità chieda al gestore del servizio di posta elettronica di duplicare la casella *e-mail* dell'indagato e di inoltrare il contenuto sui *server* della procura della Repubblica. Attesa la segretezza dell'operazione, si dovrebbe procedere, in relazione a tale situazione con le forme dell'intercettazione di flussi telematici *ex* art. 266 *bis* c.p.p.

Diversamente, vi può essere l'eventualità in cui l'apprensione del messaggio avvenga mediante sequestro a seguito di una perquisizione o ispezione dei *server* della società che gestisce il servizio o del *personal computer* dell'individuo: essendo venuta meno la segretezza, ma essendo presente la sorpresa, si sarebbe davanti ad un sequestro[147].

In questa visione, diventa relativamente problematica l'ultima eventualità accennata: quella in cui si agisca direttamente sul *device* del soggetto. Infatti in tal caso le operazioni non potrebbero essere condotte a norma degli artt. 254 e 254 *bis* c.p.p., i quali si preoccupano

[144] In tal senso si esprime, F. CERQUA, *Ancora dubbi e incertezze sull'acquisizione della corrispondenza elettronica*, in *www.penalecontemporaneo.it*, p. 7.

[145] Ci si riferisce all'opzione interpretativa fatta propria da E. M. MANCUSO, *op. cit.*, p. 70 e da F. ZACCHÈ, *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.*, 2013, n. 4, p. 109.

[146] V. sul punto, A. CAMON, *Le intercettazioni nel processo penale*, Giuffrè, Milano, 1996, pp. 22 s.

[147] Cfr. F. ZACCHÈ, *op. cit.*, p. 109.

esclusivamente del sequestro presso i gestori dei servizi di posta elettronica. La disciplina applicabile sarebbe quella del sequestro ordinario, al quale, quindi, potrebbe procedere la polizia giudiziaria[148].

Da una prospettiva analoga è stato affrontato il dibattito avente per oggetto l'acquisizione di messaggi scambiati tra *smartphone* attraverso servizi di messaggistica istantanea. In questo caso, fondamentale si è rivelato l'apporto della giurisprudenza, la quale ha ampiamente discusso circa i rapporti tra i già citati artt. 254 *bis* e 266 *bis* c.p.p.

Volendo scendere più nel dettaglio, nel caso poi diventato oggetto d'esame, si trattava di recuperare messaggi scambiati tra due terminali attraverso il sistema di messaggistica *BlackBerry Messenger*. Il programma citato permette, come è noto, lo scambio istantaneo di messaggi tra due terminali utilizzando *server* di proprietà della *Research in Motion*, società canadese proprietaria del marchio *BlackBerry* e produttrice dei medesimi *smartphone*[149].

[148] Così, F. ZACCHÈ, *op. cit.*, p. 109. L'Autore prosegue il ragionamento, prospettando possibili profili di incostituzionalità dell'art. 354, co. 2° c.p.p., il quale ammette il potere per la polizia giudiziaria di assicurazione in via d'urgenza delle fonti di prova. Tale disposizione, nell'interpretazione riferita, permetterebbe agli ufficiali di polizia giudiziaria di ottenere le *e-mail* dell'indagato, violando il disposto dell'art. 15 Cost. Infatti, la disposizione costituzionale non prevede alcun potere, nemmeno in caso di urgenza, di limitazione della libertà e segretezza della corrispondenza da parte dell'autorità di polizia. Anche F. CERQUA, *Ancora dubbi*, cit., p. 11, rileva una possibile violazione dell'art. 15 Cost. In relazione al profilo dell'estensione del potere di compressione della posizione soggettiva tutelata dall'art. 15 Cost., si rimanda alle considerazioni svolte nel Cap. III, § 5.

[149] La localizzazione in Canada dei *server* contenenti i messaggi da acquisire ha posto rilevanti problemi in tema di giurisdizione italiana e consequenziale necessità di ricorrere allo strumento delle rogatorie internazionali. La questione è stata oggetto di dibattito tanto in dottrina quanto in giurisprudenza. Quest'ultima ha ritenuto la sussistenza della giurisdizione italiana richiamandosi alla prassi esistente in tema di intercettazioni telefoniche. Infatti, la giurisprudenza maggioritaria nega la necessità di una rogatoria internazionale tutte le volte in cui la telefonata estera sia diretta ad un nodo telefonico italiano. In questo caso, proseguono i giudici di legittimità, l'attività di captazione avviene nel nostro paese, rendendo, quindi, inutile il ricorso alla rogatoria internazionale. Il medesimo ragionamento varrebbe anche nel caso di intercettazione di messaggi tra terminali *BlackBerry*. Cfr. le motivazioni di Cass. 10 novembre 2015, Guarnera, in *C.e.d.* n. 265615. Da una diversa prospettiva, la dottrina ha criticato tale impostazione partendo dal presupposto per cui l'attività di intercettazione, in realtà, non avverrebbe nel nostro Paese. Nella fattispecie considerata, infatti, difetterebbe il presupposto della presenza sul territorio nazionale di un nodo o di un *server* attraverso cui sarebbero passati i messaggi intercettati. Cfr. S. FÙRFARO, *Le intercettazioni "*pin to pin*" del sistema* BlackBerry*, ovvero: quando il vizio di informazione tecnica porta a conclusioni equivoche*, in *Arch. pen. web*, 2016, n. 1, p. 5; A. TESTAGUZZA, Chat BlackBerry*: il sistema "pin-to-pin". Nascita di un nuovo paradiso processuale*, in *Arch. Pen.*, 2016, n. 1, pp. 218 ss. Per alcune considerazioni critiche circa l'applicazione della tecnica dell'instradamento alle intercettazioni *pin to pin*, v. T. BENE, *Trasnazionalità dei crimini nella società confessionale: i pericoli della tecnologia e del diritto*, in *Giur. it.*, 2016, pp. 717 ss.

Concretamente, le autorità italiane avevano richiesto alla *Research in Motion* s.r.l., consorella italiana della società canadese, una serie di messaggi scambiati tra cellulari di persone sospettate di appartenere alla criminalità organizzata. Lo strumento utilizzato dalla magistratura inquirente, avallato dalla giurisprudenza maggioritaria, è stato quello dell'art. 266 *bis* c.p.p., sul presupposto per cui le *chat* tra utenti, pur difettando dell'immediatezza tipica delle conversazioni telefoniche, costituiscano, comunque, un flusso di carattere comunicativo[150]. Proprio il riconoscimento della natura comunicativa dei dati informatici appresi varrebbe, secondo la Cassazione, ad escludere dalla fattispecie in commento l'applicabilità degli artt. 254, 254 *bis* c.p.p.

La soluzione accolta dalla Suprema corte ha trovato l'avallo di una parte della dottrina che, sul punto, ha avuto modo di specificare meglio il ragionamento sotteso a tale scelta dogmatica. In proposito, si è sottolineato come, il sequestro si caratterizzi per avere ad oggetto dati di carattere informatico conservati e memorizzati indipendentemente dalle finalità attinenti al processo penale[151]. Alla luce di tale premessa, sarebbe corretto qualificare l'acquisizione di *chat pin to pin* come sequestro soltanto allorché i *server* della *R.I.M.* detenessero i messaggi degli utenti *BlackBerry* per questioni di utilizzo del sistema di messaggistica[152]. Non solo, sempre a parere di tali studiosi il sequestro si caratterizzerebbe per l'apprensione di materiale comunicativo ormai giunto al destinatario[153]. Per cui la linea di demarcazione tra le due fattispecie sarebbe da rintracciare nella chiusura o meno del rapporto comunicativo:

[150] Cfr. Cass. 10 novembre 2015, Guarnera, cit.

[151] Cfr. M. TROGU, *Come si intercettano le* chat pin to pin *tra dispositivi* Blackberry*?*, in *Proc. pen. giust.*, 2016, n. 3, p. 74

[152] L'idea non deve necessariamente condurre a scenari orwelliani, basti pensare all'ipotesi in cui il servizio di messaggistica mantenga sul *server* i messaggi criptati per garantirne un *backup* nel caso in cui l'utente perda o rompa il terminale.

[153] Ancora, M. TROGU, *op. cit.*, p. 74.

soltanto allorché il messaggio sia giunto sul terminale del ricevente, si potrebbe procedere tramite sequestro.

Il percorso argomentativo prescelto dai giudici di legittimità è stato, però, oggetto anche di critiche da parte di altri commentatori: al riguardo è stato rilevato come, pur essendo corretta la sottolineatura circa la particolarità dei dati appresi, risulterebbe scorretta l'equiparazione tracciata dal Supremo Collegio, tra conversazioni telefoniche e *chat*. Infatti, mentre nelle prime la comunicazione è contestuale, effettuata tra persone che si scambiano nel medesimo lasso temporale delle battute, nelle seconde il requisito della contestualità potrebbe difettare[154]. Lo scambio di messaggi non è necessariamente continuo e formato da un dialogo costante tra gli interlocutori, ma, più frequentemente, privo di una contestualità temporale. Questa mancanza di sincronicità varrebbe ad avvicinare le conversazioni effettuate tramite servizi di messaggistica alla corrispondenza, divenendone una forma particolare[155]. Non solo, da un punto di vista tecnico, la captazione non sarebbe stata effettuata in tempo reale. Le autorità inquirenti avrebbero, infatti, richiesto dati statici immagazzinati nei *server* della società proprietaria del servizio di messaggistica istantanea[156]. Queste argomentazioni condurrebbero a ritenere applicabile alla situazione descritta l'art. 254 *bis* c.p.p.

[154] V. sul punto G. PITTELLI – F. COSTARELLA, *Ancora in tema di* chat "pin to pin" *sul sistema telefonico* BlackBerry, in *Arc. pen. web*, 2016, n. 1, p. 4.

[155] In tal senso, G. PITTELLI – F. COSTARELLA, *op. cit.*, p. 2. Da un punto di vista generale, v. A. CAMON, *op. cit.*, pp. 22 s., il quale ammette la rilevanza del contesto temporale per individuare la linea di discrimine tra intercettazione e sequestro di dati informatici. Più recentemente, critica l'utilizzo di un criterio meramente temporale, S. DE FLAMMINEIS, *Le intercettazioni telematiche*, in *Dir. pen. proc.*, 2013, p. 992.

[156] Inoltre, L. FILIPPI, *Questioni nuove in tema di intercettazioni:* quid iuris *sul* "pin to pin" *dei* BlackBerry*?* in *Arch. pen. web*, 2016, n. 1, p. 3 sottolinea i possibili profili di inutilizzabilità dei dati raccolti in quanto l'intercettazione non sarebbe in ogni caso avvenuta tramite strumenti installati presso la procura della Repubblica: ciò comporterebbe una violazione dell'art. 268, co. 3° c.p.p. sanzionata dall'inutilizzabilità delle conversazioni raccolte *ex* art. 271 c.p.p. Un ulteriore aspetto critico dell'impostazione accolta dalla giurisprudenza sarebbe quello della genuinità del dato informatico raccolto, infatti, l'operazione di copiatura sarebbe stata compiuta dalla società canadese senza alcun controllo da parte dell'autorità procedente.

In conclusione, non può, però, non sottolinearsi come la tesi da ultimo esposta, seppur corretta da un punto di vista di dogmatica processuale, sembrerebbe portare ad un risultato difficilmente auspicabile. Infatti l'applicabilità dell'art. 254 *bis* c.p.p. avrebbe come effetto immediato quello di offrire una tutela meno intensa al diritto alla riservatezza e, in generale, alla segretezza delle conversazioni. L'art. 266 *bis* c.p.p. impone, infatti, l'applicazione delle medesime garanzie previste per le intercettazioni comuni, tra le quali, la presenza di una richiesta del pubblico ministero ad un giudice, la sussistenza di gravi indizi di reato, l'indispensabilità dell'atto per la prosecuzione delle indagini.

Viceversa, la normativa in tema di sequestro prevede solamente l'emanazione di un decreto motivato da parte dell'autorità giudiziaria. Accettando l'interpretazione riferita, si consegnerebbe all'autorità procedente un ampio potere di apprensione di dati che, per la loro particolarità, si situano a metà strada tra una normale conversazione telefonica e una corrispondenza epistolare. Considerando che la medesima attività comunicativa potrebbe avvenire sia attraverso una chiamata telefonica sia tramite lo scambio di messaggi, sembrerebbe irrazionale circoscrivere solo alla prima situazione l'applicabilità delle ampie garanzie previste dal codice di rito penale agli artt. 266 ss. c.p.p.

La riconduzione dell'acquisizione di messaggi scambiati attraverso terminali *Blackerry* al fenomeno delle intercettazioni di comunicazioni, non esaurisce le problematiche da affrontare. Infatti un'altra questione centrale nell'ipotesi *de qua* riguarda i mezzi utilizzati dall'autorità procedente per ottenere il contenuto delle conversazioni intercettate.

Nella vicenda giudiziaria, poi analizzata dalla cassazione nella sentenza in oggetto, le procure della Repubblica avevano agito in maniera molto simile. Ottenuta l'autorizzazione a disporre le intercettazioni, queste hanno richiesto l'aiuto della *Research in Motion* s.r.l., la quale, a sua volta, ha inoltrato la richiesta dell'autorità inquirente alla sede centrale della

Research in Motion. Sarebbe stata quest'ultima ad effettuare materialmente le attività di captazione, decriptazione e invio dei messaggi intercettati ai *server* della procura.

La procedura così descritta sembrerebbe porsi in contrasto con il disposto dell'art. 268, co. 3° e 3 *bis* c.p.p., il quale impone, salvo la sussistenza di ragioni di urgenza, che le operazioni di intercettazione siano disposte con apparecchiature localizzate presso la procura della Repubblica.

La precisazione contenuta nel co. 3 *bis* dell'art. 268 c.p.p., per cui si possono utilizzare impianti di proprietà di privata, va correttamente intesa. Al riguardo, la giurisprudenza ha chiarito come ciò che rilevi non sia il soggetto proprietario dello strumento utilizzato, ma il posizionamento della struttura al fine di garantire il corretto svolgimento delle operazioni[157]. Questa esigenza nasce, ovviamente, dalla natura delle intercettazioni e dai beni giuridici di primaria importanza che questo mezzo di ricerca della prova pone in pericolo[158]. In linea con tale assunto, viene sottolineato dalla Cassazione come le attività sarebbero state compiute attraverso le strumentazioni presenti nella procura della Repubblica, in quanto i dati sarebbero stati riversati in originale sui *server* della stessa[159]

In questo quadro, come anche rilevato dalla dottrina, le modalità scelte dalla procura della Repubblica nella fattispecie *de qua* per ottenere copia delle *chat* sembrerebbero porsi in contrasto con quanto appena riferito[160]. L'intera struttura utilizzata per la captazione si trova, infatti, in Canada; le attività di copiatura e decifratura sono state svolte in autonomia dalla società canadese.

---

[157] V. in tal senso, le motivazioni di Cass. sez. I, 19 dicembre 2014, Terracchio, in *C.e.d.* n. 262485.

[158] Per alcuni spunti in tal senso, v. D. NAIKE CASCINI, *Messaggistica tra telefonia* Blackberry*: nuove prassi devianti al limite dell'abuso del processo*, in *Arch. pen. web*, 2016, n. 2, pp. 4 s.

[159] Cfr., in motivazione, Cass. sez. III, 29 gennaio 2016, Rao, in *C.e.d. cass.* n. 266490.

[160] Cfr. D. NAIKE CASCINI, *op. cit.*, p. 4; M. TROGU, *op. cit.*, p. 75.

Come sottolineato da alcuni studiosi, in tal modo i giudici di legittimità sembrerebbero aver parificato l'attività di captazione dei messaggi con quella di trasmissione degli stessi sui *computer* dell'autorità requirente[161].

Emerge ancora una volta la difficoltà di conciliare gli istituti propri della normativa processuale con l'emergere delle nuove tecnologie. Infatti la natura ibrida delle conversazioni che avvengono attraverso i più comuni sistemi di messaggistica pone in crisi l'interprete che voglia ricondurre ad armonia il sistema[162].

[161] V. in tal senso, A. TESTAGUZZA, Chat BlackBerry*: il sistema "*pin to pin*". Nascita di un nuovo paradiso processuale*, in *Arch. pen.*, 2016, n. 1, p. 218.

[162] La situazione descritta rischia, almeno nell'immediato futuro, di complicarsi ulteriormente a causa di alcune innovazioni tecniche che stanno emergendo nel mondo dei programmi di messaggistica istantanea. Il riferimento è all'utilizzo di strumenti di crittografia c.d. *end to end*. Grazie a questo sistema di criptazione soltanto le persone che stanno comunicando sono in grado di leggere in chiaro il testo del messaggio che si stanno scambiando. La diffusione di tale metodologia rende, nei fatti, estremamente difficile l'attività di intercettazione compiuta nelle sentenze precedentemente citate. Infatti, i sistemi di criptazione *end to end* rendono il messaggio illeggibile sia per i fornitori di connettività che per i fornitori del servizio di messaggistica. Per dare un'idea dell'estensione del fenomeno, si tenga conto del fatto che recentemente uno dei più popolari sistemi di messaggistica istantanea, *WhatsApp*, ha deciso di implementare la crittografia *end to end*. L'annuncio è stato dato sul *blog* della società *Open Whisper System*, sviluppatrice di un importante *software* di crittazione *end to end*: https://whispersystems.org/blog/whatsapp/

Capitolo V

Le prove informatiche di carattere "atipico"

SOMMARIO: 1. Le c.d. perquisizioni on-line – 2. L'utilizzo del captatore informatico – 3. (segue): le ipotesi di riforma – 4. I dispositivi di geolocalizzazione

1. Le c.d. perquisizioni *on-line*

Nel capitolo precedente si sono affrontate le questioni afferenti alle prove informatiche c.d. "tipiche". Con questa espressione si è fatto riferimento a tutti quegli strumenti di prova che trovano una specifica regolamentazione nell'àmbito della normativa processuale, in quanto riconducibili a istituti già noti ovvero disciplinati *ad hoc*. Viceversa, il presente capitolo avrà ad oggetto le prove informatiche c.d. "atipiche", ossia quelle fonti conoscitive di carattere informatico che, allo stato, non sono direttamente riconducibili agli istituti del codice di procedura penale.

Tra queste rivestono un ruolo estremamente importante le c.d. perquisizioni *on-line*, categoria eterogenea all'interno della quale possono essere ricomprese diverse tecniche di indagine. Volendo tentare di fornire una prima descrizione generale di tali strumenti, si può affermare come questi siano caratterizzati dall'utilizzazione da parte dell'autorità inquirente di *software* malevoli capaci di attivare determinate periferiche di uno strumento elettronico, di registrare tutte le attività effettuate da un utente tramite lo stesso o di effettuare copia dei

dati contenuti nel *device* analizzato[1]. Si tratta, con tutta evidenza, di un mezzo estremamente versatile, capace di compiere diverse attività investigative, le quali, a loro volta, possono essere accostate a diverse categorie processuali.

Per cogliere l'importanza dell'utilizzo di tali strumentazioni può essere utile riflettere sull'ormai costante uso da parte della criminalità, organizzata e non solo, di mezzi di comunicazione criptati, i quali possono essere oggetto di intercettazione solo attraverso i *software* cui si fa riferimento. In tal senso, alcuni hanno, inoltre, affermato come la disponibilità di questi metodi investigativi costituirebbe «più che un potenziamento, un recupero della efficacia "perduta"[2]».

La dottrina ha cercato di proporre una prima suddivisione di massima a cui si intende aderire, inquadrando il fenomeno in discorso in due categorie: da un lato l'*on-line surveillance* e, dall'altro, l'*on-line search*[3]. Con la prima espressione si fa riferimento a quelle operazioni di sorveglianza costante dell'elaboratore "bersaglio" al fine di ottenere informazioni riguardati i siti *web* visitati, le *e-mail* inviate o al fine di attivare una delle periferiche del dispositivo. Diversamente, il secondo termine ha per oggetto le tecniche che permettono di estrarre dal *computer* del soggetto controllato i singoli *file* presenti sullo stesso[4]. Al fine di mantenere un certo ordine nell'esposizione, il presente paragrafo tratterà esclusivamente

[1] Per una panoramica di carattere tecnico-divulgativo di tali strumenti, v. M. ZONARO, *Il Trojan – Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento d'intercettazione*, in *Parola alla difesa*, 2016, pp. 163 ss.

[2] Così, E. PIO, *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite*, in *Parola alla difesa*, 2016, pp. 161 s.

[3] Cfr. R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgeright *sulla c.d.* online durchsuchung, in *Riv. trim. dir. pen. econ.*, 2009, p. 696. Per una panoramica internazionale del tema, v. P. LE FÈVRE, *Il regime della captazione dei dati informatici nel diritto francese*, in *Parola alla difesa*, 2016, pp. 181 ss.; F. IOVENE, *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont.*, 2014, nn. 3-4, pp. 330 ss.; P. DE SÁ – C. LEONOR CHASTRE, *L'utilizzo del captatore informatico "Trojan Horse" nella procedura penale portoghese*, in *Parola alla difesa*, 2016, pp. 183 ss.

[4] V., ancora, R. FLOR, *op. cit.*, pp. 696 per alcuni riferimenti bibliografici di carattere tecnico su entrambe le metodologie di controllo.

delle tecniche dell'*on-line search*, lasciando, invece, le questioni afferenti alle attività di *on-line surveillance* ai paragrafi successivi.

Il punto di partenza della trattazione è rappresentato da una pronuncia della Corte costituzionale tedesca, la quale è stata tra le prime ad occuparsi del tema. Questa sentenza, anche se emanata da un organo straniero, presenta rilevanti profili di interesse per l'analisi del tema delle perquisizioni *on-line*, contenendo, come si vedrà meglio più avanti, i punti cardini della tematica[5]. La questione di legittimità costituzionale aveva ad oggetto la legge sulla protezione della Costituzione del North Rhein Westfalia, la quale prevedeva la possibilità per un organismo di *intelligence* di effettuare alternativamente un monitoraggio segreto di *Internet* o l'accesso segreto ad un sistema informatico[6].

La particolarità per cui merita di essere segnalata questa pronuncia è il modo in cui viene affrontata la questione dei diritti lesi dalla normativa citata[7]. Infatti dopo aver fatto riferimento agli articoli della Costituzione tedesca che hanno per oggetto rispettivamente la tutela delle comunicazioni e l'inviolabilità del domicilio, i giudici costituzionali chiamano in causa il diritto fondamentale alla garanzia dell'integrità dei sistemi informatici e della riservatezza dei dati ivi contenuti[8]. Questa posizione soggettiva costituisce un profilo del più generale diritto della personalità. Secondo la Corte costituzionale tedesca il diritto citato viene in gioco tutte le volte in cui vi sia il pericolo che gli strumenti investigativi possano portare

[5] Si fa riferimento alla sentenza BVerfG 370/2007-595/2007, 27 febbraio 2008, in *Computer und Recht*, 2008, pp. 306 ss., trad. it. parziale a cura di R. FLOR, *La sentenza del* Bundesverfassungsgeritcht *del 27 febbraio 2008 sulla c.d.* online durchsuchung, in *Riv. trim. dir. pen. econ.*, 2009, pp. 679 ss.

[6] Più precisamente, la questione aveva ad oggetto i §§ 5, co. 2, n. 11; 7, co .1; 5, co. 3, 5, co. 1 e 13 della legge sulla protezione Costituzione del North Rehin Westfalia così come modificata il 20 dicembre 2006. Il § 5 co. 2, n. 11 autorizzata un organismo di *intelligence*, operante a difesa della Costituzione, ad effettuare, alternativamente o il monitoraggio e la ricognizione segreti di *internet* oppure l'accesso segreto a sistemi informatici.

[7] Cfr. M. TORRE, *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. proc.*, 2015, p. 1169.

[8] V., sul punto, F. IOVENE, *op. cit.*, pp. 336 s.

ad una conoscenza rilevante di parti significative della vita di una persona. Inoltre tale diritto si caratterizza per essere di estrema rilevanza così da dover essere posto, pertanto, in bilanciamento con le esigenze di repressione dei reati e di tutela della collettività.

In tale contesto, acquista centralità, tra gli altri, anche il principio di proporzionalità, il quale impone che le limitazioni ai diritti fondamentali debbano perseguire uno scopo legittimo ed essere idonee come mezzo per il raggiungimento dello stesso[9]. Sotto il primo profilo, costituisce sicuramente una finalità legittima la difesa dello Stato. Tuttavia, sempre nell'ottica di un giusto equilibrio tra esigenze opposte, la minaccia per la collettività deve essere particolarmente seria. Solo una tale situazione può giustificare una normativa che permetta all'autorità di raccogliere un gran numero di informazioni personali. In altri termini, lo strumento in discorso deve costituire una sorta di *extrema ratio* per l'ordinamento, adottabile solo allorché non sia possibile ricorrere a diversi strumenti di indagine meno invasivi.

Venendo in gioco diritti di carattere fondamentale, assume rilevanza anche il tema del controllo nell'uso di tali metodologie di indagine da parte dell'autorità. Proprio per questo motivo, proseguono i giudici costituzionali tedeschi, è necessario che sia disegnata con precisione la fattispecie applicativa delle perquisizioni *on-line*, stabilendo da un lato, i reati per i quali possa essere impiegata e, dall'altro, le modalità di utilizzo della stessa[10].

[9] Come fatto notare da G. SCHENA, *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*, in *Cass. pen.*, 2016, pp. 297 s., il principio di proporzionalità in materia di prove informatiche è stato recentemente citato dalla stessa Corte di cassazione nelle motivazioni di Cass. sez. VI, 24 febbraio 2015, Rizzo, in *C.e.d.* n. 264092.

[10] Tramite la sentenza BVerfG 966/09 - 1140/09, 20 aprile 2016, in https://www.bundesverfassungsgericht.de, la Corte costituzionale tedesca ha avuto modo di ritornare sul tema ribadendo, nella sostanza, l'orientamento prima riassunto. Per un commento in lingua italiana alla pronuncia, v. L. GIORDANO – A. VENEGONI, *La corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *www.penalecontemporaneo.it*

Rivolgendo lo sguardo adesso al nostro Paese, la prospettiva, almeno al momento, cambia radicalmente. La prima pronuncia che si è occupata del tema è di poco successiva al citato arresto giurisprudenziale tedesco e presenta un approccio nettamente diverso al tema[11].

Nell'àmbito di un procedimento iniziato per il pubblico ministero con decreto, aveva autorizzato l'installazione di un *trojan* sul *computer* di uno degli indagati al fine di ottenere copia non solo dei documenti già formati ma anche di quelli elaborandi[12]. La difesa dell'imputato, nel ricorso presentato avverso la sentenza di condanna, aveva sostenuto che tale operazione fosse, invece, da qualificare come intercettazione di flussi informatici *ex* art. 266 *bis* c.p.p., essendo ininfluente ai fini della qualificazione dell'atto il numero di soggetti attinti dal mezzo di ricerca della prova. Secondo la prospettazione del ricorrente, anche nel caso in cui vi fosse un solo soggetto interagente col sistema informatico, si dovrebbe ricadere nella categoria delle intercettazioni.

La Corte di cassazione rigetta le argomentazioni della difesa, sostenendo che lo strumento impiegato dagli inquirenti va qualificato come prova atipica *ex* art. 189 c.p.p. In primo luogo, viene esclusa l'ipotesi che si tratti di intercettazione di flussi di dati, in quanto ad essere captato era stato un flusso unidirezionale di dati. In secondo luogo, si ammette la possibilità che tale strumento di indagine possa essere autorizzato dal semplice decreto del pubblico ministero. Sul punto la Corte, in maniera relativamente frettolosa, esclude che nell'operazione condotta vi sia stata una violazione degli artt. 14, 15 Cost. Rispetto al primo profilo,

[11] Cfr. Cass. sez. V, 14 ottobre 2009, Virruso ed altri, in *C.e.d. cass.* n. 246954.

[12] Il termine *trojan horse*, talvolta abbreviato in *trojan*, significa letteralmente cavallo di Troia in analogia con lo stratagemma utilizzato dagli achei contro i troiani per vincere la guerra di Troia. Il parallelismo deriva dal funzionamento stesso dello strumento. È l'utente, infatti, che, in maniera inconsapevole, installa il *trojan* sul proprio elaboratore. Lo strumento in discorso può essere utilizzato non solo per intercettare comunicazioni tra presenti, ma anche per individuare la refurtiva di un furto. Questa è l'eventualità studiata da F. MORELLI, *Videoriprese mediante la* webcam *di un computer illecitamente sottratto e tutela del domicilio*, in *Dir. pen. proc.*, 2013, pp. 475 ss.

si fa notare come ciò che è stato appreso non sia il contenuto di una comunicazione. I *file* conservati nell'*hard disk* erano semplici documenti di testo che non costituiscono, in quanto tali, corrispondenza. Sotto l'aspetto della tutela del domicilio, i giudici di legittimità affermano come l'elaboratore in uso all'imputato fosse installato all'interno di un ufficio pubblico, nel quale, secondo le cadenze stabilite dagli orari, era ammesso l'ingresso di persone estranee. In questo senso, l'imputato non poteva vantare alcun diritto alla riservatezza stante la natura di luogo aperto al pubblico dell'ufficio in cui era ubicato il *computer*.

La dottrina non ha mancato di rilevare come l'apparato motivazionale dei giudici di legittimità appaia sotto certi aspetti criticabile[13]. Tra i vari profili toccati dai giudici di legittimità, quello riguardante l'inviolabilità del domicilio è stato il più contestato. Si sottolinea, infatti, come il legislatore stesso abbia riconosciuto l'esistenza di quello che viene comunemente definito il c.d. domicilio informatico[14]. Con questa espressione si fa riferimento alla sussistenza di una sfera privata di riservatezza contenuta all'interno dell'elaboratore. L'idea sottesa è quella dell'analogia tra il domicilio in senso fisico e quello virtuale: entrambi meritano protezione in quanto costituiscono una proiezione della personalità del soggetto[15]. In quest'ottica, alla luce anche del carattere personalissimo delle informazioni che possono essere contenute all'interno di un *device* elettronico, si ritiene che il semplice decreto del pubblico ministero non costituisca una garanzia sufficiente. Infatti, l'art. 14 Cost., sotto cui dovrebbe ricadere anche la tutela del domicilio informatico, impone la doppia riserva di legge

[13] In tal senso, v. A. TESTAGUZZA, *I Sistemi di Controllo Remoto: fra normativa e prassi*, in *Dir. pen. proc.*, 2015, p. 765; M. TORRE, *op. cit.*, p. 1165.

[14] Sul punto si richiamano le considerazioni svolte nel Cap. III, § 4.

[15] V. in relazione alla citata sentenza, F. PERNA, *Il captatore informatico nell'attuale panorama investigativo: riflessi operativi*, in *Parola alla difesa*, 2016, p. 170; M. TORRE, *op. cit.*, p. 1166.

e di giurisdizione. Nel caso in discorso entrambe queste previsioni risultano non rispettate, con la conseguente inutilizzabilità del materiale raccolto[16].

Sul punto, merita, però, di essere rilevato come alcuni si spingano ancora più in avanti sul tema delle posizioni soggettive lese da tale strumento[17]. Infatti il paragone giustificante la teorica del domicilio informatico, come illustrato precedentemente, sembrerebbe non reggere appieno. Il domicilio sarebbe pur sempre caratterizzato da una sua fisicità, elemento che, per sua natura, manca allorché si faccia riferimento al domicilio informatico[18]. Inoltre, quest'ultimo non sembrerebbe essere lo strumento più adatto per una protezione completa dell'individuo. Il punto focale del tema dovrebbe essere rappresentato dalla nozione di riservatezza informatica, la quale, appunto, pone al centro non l'esistenza o meno di luoghi virtuali, ma la necessità di proteggere i dati in quanto tali[19].

Proprio per quanto attiene alla qualificazione giuridica delle attività di *on-line search*, alcuni studiosi hanno rimarcato la difficile compatibilità tra queste e l'ordinamento italiano. Infatti, tali misure, caratterizzate dall'essere predisposte all'insaputa del soggetto sottoposto ad indagine, sembrerebbero costituire una modalità per aggirare le disposizioni del codice di rito penale finalizzate alla tutela dei diritti di difesa[20]. Ciò in quanto, attraverso un *trojan*

[16] Ancora, M. TORRE, *op. cit.*, p. 1167.

[17] Si fa riferimento a P. FELICIONI, *L'acquisizione di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. giust.*, 2016, n. 5, p. 126.

[18] Cfr. R. ORLANDI, *Osservazioni sul documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici*, disponibile su *www.archiviopenale.it*

[19] V. Cap. III, § 3. Sempre nel medesimo periodo temporale a cui si riferisce la pronuncia della Cassazione testé analizzata, la questione era stata affrontata dal giudice per le indagini preliminari presso il Tribunale di Napoli. In tale procedimento, instaurato a carico degli appartenenti alla presunta associazione di stampo massonico denominata P4, il captatore utilizzato dagli investigatori era programmato a svolgere una duplice la funzione sia di *on-line search* sia di *on-line surveillance*. Sotto il primo profilo, l'operazione veniva ricondotta nell'alveo delle intercettazioni di flussi informatici di cui all'art. 266 *bis* c.p.p., per il secondo aspetto, essa, invece, veniva qualificata come attività di indagine atipica per la quale doveva considerarsi sufficiente un decreto del pubblico ministero. Uno stralcio del provvedimento del giudice per le indagini preliminari presso il Tribunale di Napoli che affronta la questione può essere letto in M. TORRE, *op. cit.*, p. 1167, nt. 21.

[20] Così, M. TORRE, *op. cit.*, p. 1171.

si potrebbero ottenere le medesime informazioni acquisibili attraverso i normali atti di perquisizione ed ispezione previsi dal codice di procedura penale. Attività questa che consente, però, un più corretto bilanciamento tra il diritto di difesa della persona sottoposta alle indagini e le esigenze di repressione dei reati. Secondo altri, disposti su di una linea argomentativa più morbida, si potrebbero equiparare le *on-line search* alle normali perquisizioni: entrambi gli atti perseguirebbero lo scopo di prendere possesso di una *res* digitale, l'unica differenziazione sarebbe costituita dalle modalità di apprensione dell'elemento probatorio[21]. Ovviamente la riconduzione delle perquisizioni *on-line*, almeno per quanto attiene il profilo dell'estrazione di documenti informatici, al mezzo di ricerca della prova di cui agli art. 247 ss. c.p.p., comporterebbe l'estensione all'atto in discorso delle garanzie previste dal codice di rito penale[22].

In realtà entrambe le argomentazioni illustrate non appaiono del tutto convincenti. Per quanto attiene all'identità degli elementi acquisibili attraverso le *on-line search* rispetto alle normali perquisizioni, può essere precisato come le prime, caratterizzandosi per un'attività di sorveglianza continua, permettono l'individuazione di maggiori elementi probatori rispetto alle indagini "classiche". Infatti il soggetto, a causa della segretezza dell'atto, continua ad utilizzare il *device* per i propri scopi, permettendo all'autorità procedente la collezione di un numero sempre maggiore di documenti informatici.

In merito alla seconda opinione riferita, può risultare utile sottolineare come l'elemento qualificante dello strumento in discussione sia proprio la segretezza dell'atto. È tale particolarità a rendere le operazioni in commento estremamente delicate ma anche partico-

[21] In tal senso si esprime, A. TESTAGUZZA, *op. cit*, p. 764.

[22] Cfr., A TESTAGUZZA, *op. cit.*, p. 764.

larmente vantaggiose per le indagini preliminari. L'attenzione, come si avrà modo di specificare più avanti, va posta sulla ricerca di una normativa che possa fornire un giusto bilanciamento tra gli interessi in gioco: permettere l'utilizzazione di tali strumenti solo dietro un pieno controllo da parte dell'autorità giurisdizionale.

In realtà, come riferito da altra parte della dottrina, le attività di copiatura da remoto dei documenti informatici presenti su un determinato elaboratore non sono riconducibili agli istituti regolati dal codice di procedura penale[23]. Sicuramente, come precisato prima, queste operazioni si caratterizzano per la loro segretezza. Tale requisito potrebbe indurre a pensare ad un avvicinamento tra le stesse e le intercettazioni di comunicazioni. Tuttavia, una tale operazione sarebbe errata: infatti, il nucleo centrale del mezzo di ricerca della prova di cui agli artt. 266 ss. c.p.p. è costituito dalla captazione di conversazioni che avvengono tra due soggetti[24]. Nel caso delle perquisizioni *on-line*, tale requisito difetterebbe in quanto ciò che viene appreso è costituito da un documento informatico memorizzato sulla memoria dell'elaboratore[25].

Considerando che l'installazione di un *trojan* permette agli investigatori di osservare l'intero contenuto di un *computer*, si potrebbe ipotizzare un'analogia con le ispezioni. Tale similitudine, ad un'analisi più approfondita, risulta, però, solo apparente. Ciò, in quanto le finalità dell'utilizzo di un captatore informatico sono quelle di recuperare documenti e non la semplice visione del contenuto di un *device* elettronico[26].

[23] In tal senso, v. S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. pen. web*, 2014, n. 1, pp. 4 ss.; S. MARCOLINI, *Le cosiddette perquisizioni* on line *(o perquisizioni elettroniche)* in *Cass. pen.*, 2010, pp. 2859 ss.

[24] *Ex multis*, A. CAMON, *Le intercettazioni nel processo penale*, Giuffrè, Milano, 1996, pp. 16 ss.

[25] Cfr., S. MARCOLINI, *op. cit.*, p. 2859.

[26] Ancora, S. MARCOLINI, *op. cit.*, p. 2860.

Dalla breve analisi condotta, sembrerebbe più corretto ritenere allo stato l'utilizzo del c.d. *virus* di Stato per ottenere copia di dati informatici come strumento non utilizzabile nel nostro ordinamento processuale. Come argomentato anche in dottrina, le *on-line search* costituiscono, al momento, un'ipotesi di prova incostituzionale, in quanto si pongono in violazione degli artt. 14, 15 Cost.[27]. In relazione al primo, come anche in parte già chiarito, viene rilevata la mancanza di una disciplina che regolamenti dettagliatamente le operazioni di introduzione del programma spia, il quale già costituisce un'ipotesi di lesione dell'inviolabilità del domicilio[28]. In relazione al profilo della tutela del diritto di cui all'art. 15 Cost., il *vulnus* che si viene a creare riguarda un particolare profilo della libertà e segretezza delle comunicazioni che è quello della riservatezza informatica[29].

Anche il richiamo all'art. 189 c.p.p. non sarebbe risolutivo della questione, per almeno due ordini di motivazioni. Da un canto, la norma citata, proprio alla luce della sua genericità, non può essere considerata idonea a soddisfare la riserva di legge imposta dagli articoli della Costituzione cui si è fatto riferimento prima[30]. Dall'altro, va rilevato come nel caso di cui si discute, trattandosi di strumento probatorio che si pone in diretto contrasto con la tutela di alcuni diritti fondamentali previsti dalla Costituzione, il richiamo all'art. 189 c.p.p. sembrerebbe un *escamotage* per aggirare le disposizioni che proteggono il domicilio e la libertà e segretezza delle comunicazioni[31].

---

[27] Così, P. FELICIONI, *op. cit.*, 5, p. 132; M. TROGU, *Le indagini svolte con l'uso di programmi spia (*trojan horse), in *La giustizia penale nella rete*, a cura di R. Flor – D. Falcinelli – S. Marcolini, DIPLAP EDITOR, 2015, p. 71. Per la definizione dell'espressione prove incostituzionali, si rimanda a V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale*, in *Giur. cost.*, 1973, p. 341.

[28] V., sul punto, M. TROGU, *Le indagini*, cit., p. 68

[29] Ancora, M. TROGU, *Le indagini*, cit., p. 69, il quale ricollega la tutela della riservatezza informatica alla lettura combinata degli artt. 13, 14 e 15 Cost. compiuta da Corte cost., 24 aprile 2002, n. 135, in *Giur. cost.*, 2002, pp. 1062 ss.

[30] In tal senso, P. FELICIONI, *op. cit.*, p. 132.

[31] Cfr. M. TROGU, *Le indagini*, cit., p. 69.

Per le ragioni esposte, l'unica via percorribile, sulla quale si ritornerà più avanti, appare quella dell'intervento di carattere legislativo teso a regolare la fattispecie in discorso.

2. L'utilizzo del captatore informatico

Come rilevato precedentemente, una delle funzioni che può essere svolta attraverso l'installazione di particolari programmi su di un *device* elettronico è quella dell'attivazione delle periferiche audio o video al fine di trasformare gli stessi in strumenti di intercettazione di conversazioni. A prima vista, tale evenienza non sembrerebbe comportare particolari problemi applicativi, in considerazione del fatto che la tematica delle intercettazioni di conversazioni risulta compiutamente disciplinata dal codice di rito penale.

Tuttavia, ad uno sguardo più attento, l'utilizzazione di tali strumentazioni fa nascere rilevanti questioni. Occorre considerare come, attraverso l'installazione di un captatore informatico, lo strumento elettronico "infettato" si trasformi in una sorta di microspia mobile, in grado di seguire il soggetto in tutti i suoi spostamenti[32]. È proprio questa capacità di costante captazione a creare le maggiori difficoltà applicative. Il soggetto che subisce tale atto investigativo, trasportando con sé la "cimice", permette, infatti, agli investigatori di effettuare delle intercettazioni di carattere ambientale in tutti i luoghi in cui questi si reca.

Diviene, pertanto, necessario approfondire la questione riguardante la compatibilità di tali operazioni in relazione alle garanzie previste per l'effettuazione di intercettazioni di conversazioni all'interno del domicilio. Queste ultime, infatti, possono, come è noto, essere autorizzate, per i reati di cui all'art. 266 c.p.p. allorché sussistano gravi indizi di reato, siano assolutamente indispensabili per la prosecuzione delle indagini e, punto centrale del di-

[32] Secondo, A. CISTERNA, *Cedu e diritto alla privacy*, in *I princìpi europei del processo penale*, a cura di A. Gaito, Dike giuridica editrice, Roma, 2016, pp. 213 s. le caratteristiche di estrema versatilità e mobilità dello strumento andrebbe ad escludere anche la possibilità di ricondurre il captatore informatico nell'alveo delle intercettazioni ambientali.

scorso, soltanto se vi sia il fondato motivo di ritenere che all'interno del domicilio si stia svolgendo l'attività criminosa. Dal testo della disposizione emerge, quindi, la necessità di indicare preventivamente il luogo in cui deve essere installata la microspia non solo per finalità tecnico-pratiche, ma anche per questioni di tutela dell'inviolabilità del domicilio[33]. Dal canto suo, l'art. 13 d.l. 13 maggio 1991, n. 152 conv. in l. 12 luglio 1991, n. 203 ha previsto in relazione al mezzo di ricerca della prova in discorso una disciplina derogatoria applicabile nei soli procedimenti di criminalità organizzata. In tali casi, i presupposti per l'autorizzazione dell'intercettazione di comunicazioni sono meno stringenti, bastando la sussistenza di sufficienti indizi di reato e la necessità del compimento delle stesse per lo svolgimento delle indagini. Per quanto attiene allo svolgimento delle medesime operazioni all'interno del domicilio si dispone espressamente che queste sono legittime «anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa».

Come sottolineato dalla dottrina, nonostante il tema sia stato affrontato da poche pronunce, è possibile raggruppare gli arresti giurisprudenziali sul punto in tre diversi indirizzi caratterizzantesi da un diverso approccio al tema[34].

In un primo momento, la questione è stata in parte "schivata". Trattandosi, rispetto ai casi esaminati, di procedimenti in materia di criminalità organizzata, i giudici della Corte di cassazione, al fine di rigettare le istanze delle difese, hanno avuto buon gioco nell'invocare la già citata disciplina speciale di cui all'art. 13 d.l. n. 152/1991, secondo cui l'intercettazione

[33] Cfr. Cass. sez. II, 8 aprile 2014, Alvaro ed altri, in *C.e.d. cass.* n. 259255; Cass. sez. V, 6 ottobre 2011, Ciancitto, in *C.e.d. cass.* n. 252137; Cass. sez. VI, 11 dicembre 2007, Sitzia ed altri, in *C.e.d. cass.* n. 239634, le quali affermano la necessità di indicare all'interno del decreto autorizzativo delle intercettazioni ambientali il luogo in cui si svolgerà l'attività captativa, ammettendo, inoltre, che questa possa estendersi, senza la necessità di alcuna successiva autorizzazione, anche alle pertinenze dello stesso.

[34] Si fa riferimento alla ripartizione operata da A. BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen.*, 2016, p. 2276 ss. e ripresa da P. FELICIONI, *op. cit.*, pp. 133 s.

tra presenti anche nei luoghi di domicilio è consentita indipendentemente dallo svolgimento dell'attività criminosa[35].

Successivamente, si è assistito ad un cambio di prospettiva, sulla base del rilievo della imprevedibilità dei luoghi di privata dimora suscettibili di essere violati. Tale constatazione costituisce il punto di partenza di quell'orientamento che limita la possibilità per gli inquirenti di utilizzare il captatore informatico[36]. Al riguardo, si rileva come l'art. 266 c.p.p., in quanto norma che rende effettiva la tutela costituzionalmente prevista in tema di segretezza delle comunicazioni, sia di stretta interpretazione e rende obbligatorio per il pubblico ministero l'indicazione precisa del luogo sottoposto ad intercettazione ambientale. La conseguenza di tale linea argomentativa sarebbe, quindi, rappresentata dalla possibilità di utilizzazione del captatore informatico soltanto nel caso in cui il pubblico ministero sia in grado di prevedere *ex ante* i luoghi in cui si svolge l'attività captativa.

Questa lettura è stata criticata sia da un punto di vista giuridico che tecnico. In primo luogo, viene sottolineato come l'orientamento da ultimo citato non tenga in alcun conto la disciplina speciale in tema di indagini riguardati i delitti di criminalità organizzata che, come è noto, ha l'effetto di rimodulare i presupposti dell'intercettazioni nel domicilio[37]. Non solo, in proposito, non deve essere dimenticato come da un punto di vista meramente tecnico la captazione non sia costante. Infatti al fine di evitare un eccessivo consumo della batteria del *device*, eventualità che potrebbe portare il soggetto indagato o a sospettare circa la presenza di *software* malevolo o, più semplicemente, alla sostituzione dell'apparecchio, l'attivazione

[35] Cfr. Cass. sez. VI, 12 marzo 2015, Maglia, *inedita*; Cass. sez. VI, 8 aprile 2015, Cantone, *inedita*.

[36] Ci si riferisce a Cass. VI, 26 maggio 2015, Musumeci, in *C.e.d. cass.* n. 265654.

[37] G. LASAGNI, *L'uso di captatori informatici (*trojans*) nelle intercettazioni "fra presenti"*, in *www.penalecontemporaneo.it*, p. 17.

del microfono avviene dietro impulso degli inquirenti allorché si ritenga che il soggetto sia impegnato in conversazioni utili per le indagini[38].

L'ultima fase della evoluzione giurisprudenziale in esame è quella sfociata nella recentissima pronuncia della Corte di cassazione a sezioni unite, la quale ha sottolineato come l'utilizzazione del captatore informatico ai fini di registrazione di conversazioni tra presenti all'interno del domicilio sia legittima solo per i reati cui si applica la speciale disciplina di cui all'art. 13 d. l. n. 152/1991[39].

La vicenda nasce da un procedimento riguardante reati di criminalità organizzata, nel quale veniva impugnata un'ordinanza di custodia cautelare emessa sulla base delle dichiarazioni captate attraverso un *virus* informatico. Nel ricorso per cassazione, la principale argomentazione proposta dalla difesa avverso il decreto che aveva disposto le operazioni, riguardava l'indeterminatezza delle indicazioni, ivi contenute, in relazione al luogo in cui esse si sarebbero dovute svolgere. In effetti il provvedimento *de quo* conteneva un generico riferimento ai luoghi in cui si sarebbe trovato l'apparecchio portatile. La conseguenza dell'invalidità del decreto per difetto di motivazione sarebbe stata l'inutilizzabilità del materiale probatorio così ottenuto.

Questa volta la VI sezione penale della Corte di cassazione, invece di confermare l'arresto precedentemente commentato, decide di rimettere la questione alle Sezioni unite[40].

[38] V., sul punto, E. PIO, *op. cit.*, p. 161.

[39] Cfr. Cfr. Cass. sez. Un., 28 aprile 2016, Scurato, in *C.e.d. cass.* n. 266905.

[40] L'ordinanza di Cass. sez. VI, 10 marzo 2016, Scurato, in *www.penalecontemporaneo.it*.

Come precisato da alcuni studiosi, l'intervento della Corte di cassazione si caratterizza per la ricerca di un difficile e delicato punto di equilibrio tra le esigenze di legalità processuale e quelle di tutela dei diritti dei singoli[41]. La motivazione della pronuncia, volta a segnalare la complessità del tema da affrontare, si apre con una rapida carrellata delle iniziative legislative avanzate ma mai realizzate sul punto.

Successivamente, viene affrontata la questione circa la qualificazione giuridica degli atti compiuti dal pubblico ministero. Sul punto i giudici del Supremo Collegio ritengono di poter tranquillamente ricondurre l'attività di registrazione di conversazioni tra presenti attraverso l'attivazione da remoto del microfono dello *smartphone* o del *tablet* nella categoria processuale delle intercettazioni di cui all'art. 266, co. 2° c.p.p., ancorché tale attività risulti compiuta con strumenti nuovi.

Ciò detto, la Corte sottolinea, però, come il fatto che si faccia riferimento a tali atti investigativi utilizzando l'espressione intercettazioni ambientali, non dovrebbe condurre a risultati errati[42]. Se, da un lato, infatti, l'art. 266, co. 2° c.p.p. disciplina le intercettazioni tra presenti, imponendo, come è noto, quale ulteriore presupposto, allorché si debbano captare conversazioni che avvengano nel domicilio, il fondato motivo che ivi si stia svolgendo l'attività criminosa, tuttavia, sarebbe errato, dall'altro, ricavare da tale disposizione la sussistenza di un generale obbligo, sancito a pena di inutilizzabilità, di indicazione dei luoghi della captazione tutte le volte in cui questa abbia per oggetto conversazioni tra presenti. Tale obbligo non trova, infatti, fondamento né nella giurisprudenza della Corte di cassazione né in quella della Corte europea dei diritti dell'uomo[43].

[41] In tal senso, G. LASAGNI, *op. cit.*, p. 11.

[42] Sul punto, vengono riprese le argomentazioni contenute nella *Memoria per la camera di consiglio delle Sezioni Unite del 28 aprile 2016*, p. 8. Pubblicata su *www.penalecontemporaneo.it*.

[43] Cfr. *Memoria*, cit., pp. 13 ss. Per una generale ricognizione del contenuto dell'art. 8 C.e.d.u., v. Cap. III, § 3.

Ciò che deve essere precisato, continuano i giudici del Supremo Collegio, è l'inesistenza di una generale preclusione allo svolgimento di un'attività di intercettazione attraverso un dispositivo mobile che sia in grado di seguire il soggetto che subisca tale atto.

Successivamente, viene sottolineato come, in relazione alla vicenda che ha originato il ricorso, non possa non farsi riferimento alla disciplina dettata dal legislatore per i reati di criminalità organizzata. Questa, infatti, ammette la possibilità di disporre un'intercettazione di conversazioni tra presenti in qualsiasi luogo, senza richiedere, per il caso in cui ciò avvenga in contesti peculiari, come il domicilio, particolari condizioni.

L'unione di queste due linee argomentative porta alla soluzione della questione abbracciata dalle Sezioni Unite. Innanzitutto, si riconosce il divieto di utilizzazione del captatore informatico per le indagini riguardati i reati di cui all'art. 266 c.p.p. Questo risultato sarebbe una conseguenza obbligata alla luce del disposto dell'art. 266, co. 2° c.p.p., il quale impone al pubblico ministero di argomentare in relazione al fondato motivo che nel domicilio in cui si svolgeranno le operazioni si sta compiendo l'attività criminosa. Tuttavia, tale condizione risulta impossibile da soddisfare nel caso sia adoperato un captatore informatico a causa della natura fisiologicamente itinerante della captazione.

Ben diverso è il quadro allorché il procedimento penale abbia per oggetto reati di criminalità organizzata. In tale evenienza entra in gioco la già citata disciplina speciale di cui all'art. 13 d.l. n. 152/1991, la quale espressamente ammette il potere di disporre intercettazioni di conversazioni tra presenti nel domicilio senza la necessità di preventiva individuazione di tali luoghi e prescindendo dalla dimostrazione che ivi si stia svolgendo l'attività criminosa[44]. Questa norma, costituendo una deroga all'art. 266, co. 2° c.p.p., fa cadere l'ostacolo

[44] Le Sezioni Unite, da ultimo, affrontano la questione riguardante la definizione dei reati di criminalità organizzata. Sul punto, viene richiama la definizione accettata da Cass. sez. Un., 22 marzo 2005, Petrarca, in *Cass. pen.*,

che si frapponeva all'utilizzabilità del captatore informatico nelle indagini ordinarie e lo rende legittimo nei procedimenti penali riguardanti reati di criminalità organizzata.

La sentenza in discorso, portando alla luce una tematica rimasta relativamente sommersa fino ad allora, ha suscitato numerosi commenti e reazioni. In merito alle seconde, va segnalato l'appello rivolto al legislatore, da parte di un certo numero di docenti universitari, affinché la questione circa l'utilizzo del c.d. *trojan* di Stato sia oggetto di una piena regolamentazione che possa fornire un corretto bilanciamento dei princìpi costituzionali e convenzionali coinvolti[45].

Per quanto riguarda i commenti, vi è chi ha apprezzato la pronuncia citata in quanto essa sembrerebbe fare riferimento al c.d. principio di neutralità tecnica. Sotteso a tale canone vi è l'idea per cui l'attenzione del legislatore dovrebbe porsi non tanto sui singoli strumenti tecnici che possono ledere diritti fondamentali, ma, piuttosto, sulla ricerca di moduli normativi generali idonei a tutelare questi ultimi[46]. Questa prospettiva sembrerebbe essere la migliore per un duplice ordine di motivazioni. In primo luogo, sarebbe quella maggiormente in linea con le indicazioni del legislatore europeo[47]. Infatti, la recentissima direttiva 2016/680/UE, in tema di protezione dei dati personali, espressamente afferma che «la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate». In secondo luogo, questa sarebbe quella più fruttuosa in un'ottica di lungo periodo. Infatti, indipendentemente dalla rapida evoluzione

2005, pp. 2916 ss., con nota di G. MELILLO, *Appunti in tema di sospensione feriale dei termini relativi a procedimenti per reati di criminalità organizzata*.

[45] L'appello è consultabile su *www.penalecontemporaneo.it*.

[46] Così, G. LASAGNI, *op. cit.*, p. 11.

[47] V., ancora, G. LASAGNI, *op. cit.*, p. 12.

tecnologica, vi sarebbe un efficace apparato normativo in grado di evitare che la tecnica possa andare a ledere bene giuridici di sicura natura costituzionale e convenzionale.

Inoltre, vengono da altri sottolineate la «prudenza e serietà» della pronuncia, attraverso la quale la Corte di cassazione avrebbe svolto al meglio la sua funzione nomofilattica[48]. Eventuali critiche riguardanti la parzialità dell'analisi del fenomeno del captatore informatico andrebbero ricondotte non ad un errore della Corte, quanto, piuttosto, alla delimitazione della questione sollevata[49].

Sul versante opposto si pone chi ha rilevato alcune lacune nell'*iter* motivazionale della Corte di cassazione. Il punto principale di tale critica ha ad oggetto la mancata presa in considerazione del momento di installazione del captatore informatico. In questa prospettiva si rimarca come sulla base della lettura combinata degli artt. 2, 13, 14 e 15 Cost., tutte le attività intercettative debbano essere controllate e controllabili[50]. Nel caso deciso dalla Corte di cassazione, tale requisito difetterebbe in quanto né il decreto autorizzativo del giudice per le indagini preliminari né il decreto esecutivo delle operazioni redatto dal pubblico ministero hanno documentato le attività compiute al fine di "infettare" il dispositivo bersaglio. Tale carenza si pone in contrasto con quanto espressamente prevede il codice di rito all'art. 267, co. 3° c.p.p., costituendo sicuramente un'anomalia che rende impossibile la ricostruzione dell'attività svolta nonostante la pregnanza e la rilevanza dei diritti coinvolti[51].

---

[48] Così, P. FELICIONI, *op. cit.*, p. 134.

[49] A parere di L. G. VELANI, *Trojan horse, strumenti investigativi e diritti fondamentali: alla ricerca di un difficile equilibrio*, in *Parola alla difesa*, 2016, p. 175, i giudici di legittimità avrebbero dovuto studiare in maniera più approfondita il tema in tutte le sue applicazioni. Infatti, al di là delle operazioni materialmente compiute, il captatore informatico avrebbe ben potuto effettuare attività maggiormente invasive sulla legittimità delle quali sarebbe stato necessario un pronunciamento.

[50] In tal senso, A. GAITO – S. FÙRFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen. web*, 2016, n. 2, p. 16.

[51] Ancora, A. GAITO – S. FÙRFARO, *op. cit.*, p. 17.

Nel medesimo filone si inseriscono quei commentatori che registrano con preoccupazione la possibilità che attraverso la pronuncia in esame, si apra una breccia nella tutela dei diritti fondamentali dei cittadini. In primo luogo, viene segnalato come la ricognizione dei reati per i quali si possa disporre l'intercettazione a norma del citato art. 13 d.l. n. 152/1991 sconti un'eccessiva spinta verso l'ampiamento di tale elencazione[52]. Infatti il generale richiamo all'elenco contenuto nell'art. 51 co. 3 *bis*, 3 *quater* c.p.p., disposizione che ricomprende anche i delitti di stampo terroristico, sembrerebbe forzata.

In secondo luogo vi è chi allarga il ragionamento riflettendo sulla compatibilità costituzionale dello scenario fatto proprio dalle Sezioni Unite. A parere di questi studiosi, l'inviolabilità cui fa riferimento l'art. 15 Cost. comporta, tra l'altro, che l'attività captativa sia compiutamente delineata tanto dal punto di vista soggettivo che da quello oggettivo[53]. Ciò significa che l'atto dovrebbe rivolgersi verso un soggetto determinato, specificando modalità, tempi e luoghi dello stesso. Questa previsione sarebbe, in realtà, contenuta negli artt. 266 ss. c.p.p. Infatti al momento in cui viene disposta l'intercettazione, il giudice dovrebbe, nel suo decreto autorizzativo, non solo precisare il tipo di comunicazioni oggetto di captazione, ma anche se queste si svolgeranno in un luogo pubblico, aperto al pubblico o in un domicilio[54]. A sua volta, il pubblico ministero, nel decreto con cui viene disposta l'esecuzione dell'atto, dovrebbe indicare quali saranno le comunicazioni tra presenti che saranno intercettate, spe-

[52] V., sul punto, A. TESTAGUZZA, Exitus acta probat *"Trojan" di Stato: la composizione di un conflitto*, in *Arch. pen. web*, 2016, n. 2, p. 8.

[53] In tal senso, L. FILIPPI, *Il captatore informatico: l'intercettazione* ubicumque *al vaglio delle Sezioni Unite*, in *Arch pen. web*, 2016, n. 1, p. 2.

[54] Cfr., ancora, L. FILIPPI, *op. cit.*, p. 2. A parere di L. G. VELANI, *op. cit.*, p. 178 anche nei procedimenti riguardanti delitti di criminalità organizzata non si potrebbe evitare l'indicazione del luogo in cui dovrebbe svolgersi l'attività captativa. Infatti, vi deve in ogni caso essere un collegamento tra «captazione della conversazione, utilità della medesima e luogo dove avviene l'intercettazione ambientale».

cificando anche il luogo in cui tali operazioni saranno compiute. Qualsiasi attività intercettativa compiuta al di fuori di tali regole, non potrebbe dirsi rispettosa dell'art. 15 Cost. e renderebbe i risultati ottenuti inutilizzabili[55].

Inoltre, sempre a parere dei medesimi autori, sembrerebbe che non tutte le potenzialità del *Trojan* siano state affrontate dalla Corte di cassazione. Il riferimento corre principalmente al pericolo che tale strumento possa violare rilevanti divieti di carattere probatorio, come quello di cui all'art. 103 c.p.p. in tema di garanzie del difensore, posti a tutela di diritti fondamentali come quello dell'imputato alla difesa[56].

[55] V. anche L. G. VELANI, *op. cit.*, p. 178.

[56] Cfr. L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni Unite azzeccano la diagnosi, ma sbagliano la terapia*, in *Parola alla difesa*, 2016, p. 180.

3. (segue): le ipotesi di riforma

Indipendentemente dalle opinioni espresse circa la correttezza o meno del ragionamento fatto proprio dalla Corte di cassazione, si registra in dottrina un sostanziale accordo circa la necessità di un intervento legislativo che si occupi di fornire una disciplina organica della materia.

Sul tema, il punto di partenza non può che essere quello di individuare quale sia il bene giuridico che le operazioni di perquisizione *on-line* vanno a ledere, per poi saggiare il livello di protezione accordato allo stesso dalla Costituzione e dalla C.e.d.u.

Al riguardo, merita di essere ripresa l'impostazione di chi rinviene anche nel nostro ordinamento la sussistenza di un vero e proprio diritto alla riservatezza informatica[57]. L'argomentazione ha come punto di partenza la consapevolezza circa l'inadeguatezza del concetto di domicilio informatico a fungere da scudo protettivo per il singolo[58].

Il tema diventa, quindi, quello di superare il concetto di domicilio informatico per accedere alla nozione di riservatezza informatica.

La base giuridica di un tale diritto potrebbe derivare, come già accennato, da una lettura combinata della Costituzione e della C.e.d.u. La prima, grazie all'art. 2 Cost., apre al riconoscimento di nuovi diritti della personalità[59]. Tuttavia, questa disposizione da sola non è sufficiente, in quanto non individua quelle che sono le modalità e i limiti della pubblica autorità nella compressione dei diritti tutelati. Per tale motivo, risulta necessario porre l'attenzione sull'art. 8 C.e.d.u., il quale si occupa, nello specifico, del rispetto della vita privata[60]. A

[57] Fra i primi in tal senso, v. F. IOVENE, *op. cit.*, p. 336.

[58] V., *amplius*, Cap. III, § 4.

[59] Cfr. F. IOVENE, *op. cit.*, p. 336. Si richiamano, inoltre, le considerazioni svolte al Cap. III, § 3.

[60] In tal senso, P. FELICIONI, *op. cit.*, p. 127.

norma di tale disposizione, tre sono i requisiti che rendono convenzionalmente compatibili le interferenze nella vita privata: la previsione legislativa, il perseguimento delle finalità legittime di cui allo stesso art. 8 C.e.d.u., la necessità della misura[61]. Considerando, inoltre, il valore che la normativa convenzionale ha assunto nella gerarchia delle fonti a seguito dell'intervento effettuato dalla Corte costituzionale attraverso le c.d. sentenze gemelle[62]; non sembrerebbe impossibile assegnare al diritto alla riservatezza informatica il valore di limite all'utilizzo del captatore informatico.

Un buon punto di partenza sul tema può essere rappresentato da una recentissima proposta formulata in dottrina tendente a fornire una regolamentazione completa degli atti di indagine atipici che ledono diritti fondamentali[63]. L'idea nasce da una duplice constatazione, si rileva, da un lato, come la costante evoluzione di carattere tecnologico offra agli inquirenti sempre nuove modalità di raccolta di elementi probatori. Questi ultimi si caratterizzano, inoltre, per costituire fonti di prova irripetibili – come nel caso delle perquisizioni *on-line* – destinati in quanto tali ad essere inseriti direttamente nel fascicolo per il dibattimento. Si assiste in sostanza ad uno spostamento del baricentro del processo penale dalla fase dibattimentale a quella delle indagini preliminari. Si osserva, dall'altro lato come, a fronte dell'impossibilità per il legislatore di regolare tempestivamente l'utilizzo di tutti i nuovi strumenti di indagine, si assiste alla formazione di prassi poco ortodosse, giustificate dalla volontà di adoperare in ogni caso i nuovi ritrovati della tecnologia[64].

---

[61] Per l'interpretazione accettata dai giudici di Strasburgo circa il concetto di vita privata, si rimanda alle considerazioni del Cap. III, § 3.

[62] Cfr. Corte cost., 24 ottobre 2007, n. 348 in *Giur. cost.*, 2007, pp. 3475 ss.; Corte cost., 24 ottobre 2007, n. 349 in *Giur. cost*., 2007, pp. 3535 ss.

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

[64] Le sentenze citate in relazione alle attività di *on-line search* ne costituiscono un esempio. Inoltre, S. MARCOLINI, *Le indagini*, cit., p. 773 sottolineato come la riconduzione degli atti di investigazioni atipici al fenomeno regolato dall'art. 189 c.p.p. non sia soddisfacente. Ciò in quanto l'unico strumento di controllo previsto dalla disposizione,

Il testo dell'articolato citato si pone l'obiettivo di stabilire quelli che sono i casi ed i modi che possono portare ad una legittima violazione di un diritto fondamentale, prevedendo, inoltre, gli opportuni controlli di marca giurisdizionale e le relative sanzioni. Nell'individuazione delle posizioni soggettive tutelate, si utilizza una clausola di carattere generale che richiama non solo la Costituzione, ma anche le fonti di diritto internazionale[65]. Al fine di dare attuazione al principio di proporzionalità, si limita la legittimità di tali strumenti investigativi soltanto ai più gravi reati di cui agli artt. 51, co. 3 *bis* e 3 *quater* c.p.p.

Il sicuro pregio di tale proposta è dato dall'incentivo fornito al legislatore nell'intervenire, allorché nasca la necessità di estendere l'applicazione di determinati strumenti di indagine innovativi anche alle indagini riguardati illeciti diversi da quelli precedentemente citati[66]. Si sarebbe, in sostanza, trovato un giusto bilanciamento tra le esigenze di repressione dei reati e quelle di tutela dei diritti fondamentali.

Deve essere, infine, rilevato come all'interno di un più ampio disegno di riforma del codice di procedura penale e dell'ordinamento penitenziario, si stia, al momento, discutendo circa l'introduzione di una disciplina specifica per il captatore informatico[67]. I princìpi che dovrebbero orientare l'intervento governativo sono largamente ispirati alla pronuncia delle Sezioni Unite precedentemente commentata. Da un punto di vista generale, si impone, in primo luogo, che la registrazione sia effettuata da personale della polizia giudiziaria, che indichi l'ora di inizio e di fine di ciascuna operazione captativa. In secondo luogo, si chiarisce

---

ossia il contraddittorio sulle modalità di assunzione della prova, si svolgerebbe necessariamente *ex post*, lasciando agli inquirenti la possibilità di ledere diritti fondamentali dell'individuo.

[65] Cfr. S. MARCOLINI, *Le indagini*, cit., p. 791.

[66] Cfr., ancora, S. MARCOLINI, *Le indagini*, cit., p. 790.

[67] Si fa riferimento al d.d.l., approvato dalla Camera dei Deputati in data 23 settembre 2015 rubricato modifiche al codice penale e al codice di procedura penale per il rafforzamento delle garanzie difensive e la durata ragionevole dei processi nonché all'ordinamento penitenziario per l'effettività rieducativa della pena, A.S. 2067 al momento all'esame del Senato. Per un primo commento alla riforma, v. G. SPANGHER, *La riforma Orlando della giustizia: prime riflessioni*, in *www.penalecontemporaneo.it*.

come i dati debbano transitare soltanto sui *server* della procura della Repubblica e che, al fine di garantire la trasparenza dei *software* utilizzati, sia emanato un decreto ministeriale contenente delle linee guida tecniche sui programmi utilizzabili.

Il disegno di legge, inoltre, distingue i procedimenti aventi ad oggetto i reati di cui all'art. 266 c.p.p. da quelli riguardanti i reati citati nell'art. 51, co. 3 *bis* e 3 *quater* c.p.p. Per i primi si ammette il potere di attivazione del captatore nel domicilio soltanto allorché ivi si stia svolgendo l'attività criminosa. Requisito che viene meno per le indagini riguardanti reati di criminalità organizzata e di terrorismo. Sempre per questi reati, inoltre, si ammette un potere di utilizzazione del captatore informatico in via d'urgenza, attraverso un decreto del pubblico ministero convalidato dall'autorità giurisdizionale.

Pur in attesa della conclusione dell'*iter* legislativo, non può non essere rilevata una certa miopia da parte del legislatore. Infatti, come evidenziato precedentemente, le attività di indagine che possono essere svolte attraverso l'installazione di un *software* malevolo su di un dispositivo elettronico sono molteplici e, allo stato, non regolate. Tra queste, il legislatore parrebbe scegliere di normare solo una delle operazioni che possono essere compiute. Viceversa, sarebbe auspicabile un intervento normativo organica che affronti la materia in tutta la sua complessità.

4. I dispositivi di geolocalizzazione

Un'altra forma di prova informatica atipica è rappresentata dalla tecnica del monitoraggio degli spostamenti del soggetto tramite un *tracker* g.p.s.[68]. Sicuramente si è davanti ad uno strumento che è in grado di porre in pericolo rilevanti beni giuridici. Esso, infatti, si caratterizza per il fatto di garantire una costanza dell'osservazione e, di conseguenza, per la capacità di assicurare un'elevata quantità di dati riguardanti le vite personali del soggetto osservato[69].

L'inquadramento dogmatico dello strumento in discorso è tutt'altro che scontato. Secondo una prima ricostruzione di marca prettamente dottrinale, il pedinamento elettronico sarebbe da ricondurre alle intercettazioni telematiche di cui all'art. 266 *bis* c.p.p. Il ragionamento si muoverebbe sulle linee dell'analogia tra l'istituto di cui al citato art. 266 *bis* c.p.p. e la tecnica di monitoraggio tramite g.p.s., per quanto attiene alla tutela dei diritti fondamentali posti in pericolo. Entrambi gli strumenti investigativi condurrebbero, infatti, ad una lesione

[68] La sigla è una abbreviazione di *NAVISTAR GPS*, ovvero *NAVigation Satellite Time And Ranging Global Position System*. Si tratta di un sistema di localizzazione di proprietà del dipartimento della difesa degli Stati Uniti d'America, pensato, inizialmente, solo per scopi militari. Altri Stati hanno costruito o stanno costruendo una propria rete similare di satelliti. In proposito merita di essere segnalato il progetto GLONASS della Federazione russa, il COMPASS della Repubblica popolare cinese e Galileo, sistema di posizionamento europeo che dovrebbe entrare in funzione nel 2019. Per una efficace analisi del funzionamento dei *Global Navigation Satellite System* si rimanda a P. PERETOLI, *Controllo satellitare con GPS: pedinamento o intercettazione?* in *Dir. pen. proc.*, 2003, pp. 93 s.

[69] L'installazione di un *tracker* g.p.s. sull'autovettura di un soggetto o su beni a questo appartenenti non va confusa con altre tecniche che possono permettere la localizzazione di una certa persona. Ci si riferisce, in primo luogo, alla tecnica del c.d. *positioning*, ossia alla possibilità di acquisire dalle compagnie telefoniche i dati di localizzazione di un certo apparecchio cellulare. Ciò è reso possibile dal fatto che la rete di telefonia mobile è formata da tante celle, di ampiezza variabile, a cui il telefono cellulare si aggancia per svolgere le proprie funzioni. Tale strumento, tuttavia, risulta essere nettamente meno preciso dell'utilizzazione di un dispositivo g.p.s., in quanto i dati telefonici permettono solo di individuare l'area in cui si trova il telefono cellulare e non la sua esatta posizione. La giurisprudenza ammette tale metodo investigativo riconducendolo alla categoria degli atti atipici della polizia giudiziaria per i quali non è necessaria alcuna autorizzazione giudiziale, v. Cass. sez. I, 13 maggio 2008, Stefanini, in *C.e.d. cass.* n. 240092. In secondo luogo, merita di essere menzionata la possibilità di attivare il modulo g.p.s. presente in quasi ogni moderno *smartphone* e di acquisire a distanza le informazioni così ottenute. Sulla possibilità di installare *software* malevolo su un *device* in uso ad un indagato al fine di ottenere elementi utili per le indagini, v. *infra.*

della riservatezza del soggetto ad essi sottoposto[70]. Non solo, la *ratio* che ha animato il Costituente nella predisposizione dell'apparato di garanzie a tutela della segretezza delle conversazioni previsto dall'art. 15, co. 2° Cost. emerge proprio alla luce dell'insidiosità e dell'invasività degli strumenti captativi. Nello stesso ordine di idee dovrebbe essere posto il problema del pedinamento elettronico: anche l'installazione di un *tracker* g.p.s. implica una lesione della riservatezza del singolo che avviene ad insaputa dello stesso, comportando, quindi, la necessità di circondare l'utilizzo di tale tecnica di opportune garanzie[71]. La conclusione del ragionamento sommariamente descritto sarebbe quella di ricondurre, attraverso un'interpretazione estensiva della normativa *de qua* ogni intercettazione di qualsiasi flusso di dati tra due dispositivi all'art. 266 *bis* c.p.p.[72].

Tale orientamento non è, tuttavia, andato esente da critiche. Pur essendo apprezzabile il fine, quello cioè di espandere l'area di operatività delle garanzie dettate dall'art. 15 Cost., il risultato raggiunto passa attraverso una discutibile riformulazione della definizione di intercettazione. La dottrina, infatti, riconduce tutta la disciplina delle intercettazioni – comprensiva, quindi, anche dell'art. 266 *bis* c.p.p. – alla tutela della segretezza delle comunicazioni tra soggetti[73]. Come già specificato precedentemente, uno degli elementi costitutivi dell'intercettazione è la captazione di una conversazione tra persone. In quest'ottica le intercettazioni telematiche svolgono la funzione di consentire l'apprensione di quei dialoghi che avvengono attraverso strumenti informatici o telematici. Tuttavia, la particolarità del mezzo prescelto, non fa venir meno l'oggetto della captazione, il quale rimane sempre uno scambio di battute

[70] Cfr. L. G. VELANI, *Nuove tecnologie e prova penale: il sistema d'individuazione satellitare g.p.s.*, in *Giur. it.*, 2003, p. 2375.

[71] Ancora, L. G. VELANI, *op. cit.*, p. 2375.

[72] In tal senso, D. IACOBACCI, *Sulla necessità di riformare la disciplina delle intercettazioni prendendo le mosse dalle esitazioni applicative già note*, in *Giust. pen.*, 2001, III, cc. 365 s.

[73] V., *ex multis*, A. CAMON, *op. cit.*, p. 16.

tra essere umani[74]. Cosa diversa è invece il pedinamento elettronico, il cui oggetto è costituito dalle coordinate g.p.s. del dispositivo utilizzato dagli investigatori. Non solo: altri hanno rimarcato un'altra differenza tra intercettazioni informatiche e monitoraggio tramite g.p.s. riguardante il segnale captato. Mentre, infatti, nel primo caso, ciò che si intercetta è un flusso privato di dati, finalizzato ad essere utilizzato esclusivamente dai soggetti della comunicazione; viceversa, nel caso del monitoraggio g.p.s. si accede ad un segnale pubblico, utilizzato da chiunque abbia un dispositivo idoneo allo scopo[75].

Secondo un altro orientamento, il pedinamento elettronico in mancanza di un'apposita disciplina normativa, potrebbe essere assimilato all'ispezione personale[76]. Infatti il *tracker* g.p.s sarebbe riconducibile ad una sorta di strumento di osservazione elettronica del soggetto monitorato[77]. Il pregio di una tale singolare opzione interpretativa sarebbe quello di sottoporre le attività in discorso alla emanazione da parte del pubblico ministero di un decreto motivato. Tuttavia, a ben vedere, l'analogia risulta forzata sotto diversi punti di vista. In primo luogo, il pedinamento elettronico non consente alcuna osservazione di persone, luoghi o cose. Tutt'al più permette alla polizia giudiziaria di conoscere l'esatta ubicazione del soggetto sorvegliato, senza, però, fornire alcuna indicazione visiva circa il luogo in cui il soggetto si trova. In secondo luogo, le garanzie di cui all'art. 13 Cost. che si connettono alle ispezioni sono finalizzate a garantire la libertà personale di chi subisce l'atto. In quest'ottica, si

[74] V. sul punto, G. Di Paolo, *Prova informatica (diritto processuale)*, in *Enc. dir.*, Giuffrè, Milano, 2013, ann. VI, p. 744.

[75] In tal senso, S. Signorato, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.*, 2012, p. 584.

[76] V. L. Carli, *Le indagini preliminari nel sistema processuale penale: accusa e difesa nella ricerca e predisposizione della prova penale*, Giuffrè, Milano, 2° ed., 2005, p. 333.

[77] L'Autore focalizza in realtà la sua attenzione sul diverso tema delle videoriprese in ambiente privato. Sottolineata l'analogia tra queste ultime e l'ispezione, in quanto in entrambi i casi vi sarebbe una osservazione di cose, persone o luoghi; un'attività di documentazione dell'atto e l'utilizzazione di una strumentazione idonea alla registrazione dell'attività; questi ritiene di poter estendere il proprio ragionamento anche all'attività di pedinamento elettronico. Cfr. L. Carli, *op. cit.*, pp. 322 ss.

deve evidenziare come la persona pedinata non veda in alcun modo ristretta la propria libertà personale, in quanto, vista la necessità di procedere all'insaputa dello stesso, viene a mancare qualsiasi attività di carattere coercitivo[78].

Da parte sua, la giurisprudenza risulta compatta nell'inquadrare il monitoraggio attraverso g.p.s. nell'attività d'indagine atipica svolta dalla polizia giudiziaria. In questo senso il pedinamento elettronico costituirebbe solo una particolare modalità di svolgimento del più tradizione atto del pedinamento[79]. Decisiva in tal senso, sarebbe la considerazione per cui la polizia giudiziaria non capterebbe alcuna conversazione o comunicazione tra soggetti, limitandosi, invece, a registrare la posizione sul territorio del soggetto sottoposto a tale strumento di indagine. Ammettendo un tale rapporto di genere a specie, si uniformerebbe la disciplina dei due atti, per cui il pedinamento elettronico potrebbe essere compiuto da parte della polizia giudiziaria anche di propria iniziativa senza alcuna autorizzazione del pubblico ministero.

Questo orientamento giurisprudenziale è stato criticato da gran parte della dottrina. Infatti considerando che l'utilizzo di un *tracker* g.p.s. permette un controllo costante e preciso del soggetto, sembrerebbe inopportuno affidare un mezzo investigativo così invasivo alla piena disponibilità della polizia giudiziaria[80]. Tuttavia, in senso opposto, è stato osservato come il pedinamento classico e quello elettronico non differiscano eccessivamente, in quanto entrambe le metodologie presentano vantaggi e svantaggi da controbilanciare. Infatti, pur

[78] S. SIGNORATO, *op. cit.*, p. 585.

[79] Cfr. Cass. sez. II, 13 febbraio 2013, Badagliacca ed altri, in *C.e.d. cass.* n. 255542; Cass. sez. IV, 27 novembre 2012, Lleshi ed altri, in *ivi*, n. 253953; Cass. sez. VI, 12 dicembre 2007, Sitzia ed altri, *ivi*, n. 239635.

[80] V. A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005, p. 633.

nella sua invasività, il pedinamento elettronico non consente di osservare direttamente il soggetto, impedendo agli inquirenti di annotare eventuali incontri o scambi di oggetti[81].

Alla luce di queste osservazioni e in attesa di un eventuale intervento chiarificatore del legislatore, l'opzione interpretativa prescelta dalla giurisprudenza sembrerebbe quella più opportuna[82].

[81] S. SIGNORATO, *op. cit.*, p. 589.

[82] Nello stesso senso, A. LARONGA, *L'utilizzabilità probatoria del controllo a distanza eseguito con sistema satellitare g.p.s.*, in *Cass. pen.*, 2002, p. 3052; S. SIGNORATO, *op. cit.*, p. 588. Discorso differente, deve essere compiuto per quanto attiene alle attività preparatorie alla captazione del segnale g.p.s. Infatti, allorché il *tracker* debba venir posizionato all'interno di un'autovettura, potrebbero sorgere problemi in ordine alla tutela del domicilio, non mancando opinioni favorevoli al riconoscimento della natura di domicilio privato all'abitacolo di un'automobile. Qualora fosse ammessa tale equiparazione, un'eventuale installazione di un dispositivo g.p.s. da parte della polizia giudiziaria, potrebbe comportare un'indebita compressione dell'inviolabilità del domicilio prevista dall'art. 14 Cost. Sul punto, nonostante le voci critiche della dottrina, la giurisprudenza sembra essere orientata, in senso uniforme, nella direzione del disconoscimento del valore di privata dimora all'abitacolo dell'autovettura. L'argomentazione principale ruota attorno alla considerazione per cui l'abitacolo non è fornito dei mezzi tipici atti a garantire la possibilità di risierdervi in modo stabile e continuato. Cfr., tra le tante, Cass. sez. V, 22 aprile 2014, Toma, in *C.e.d. cass*. n. 260760. In dottrina, sull'ammissibilità dell'installazione di un *tracker* g.p.s. sull'autovettura di un soggetto, si rimanda a A. LARONGA, *op. cit.*, pp. 3055 ss.; P. PERETOLI, *op. cit.*, pp. 97 s.; L. G. VELANI, *op. cit.*, pp. 2373 s.

Osservazioni conclusive

Il tema della prova di carattere informatico costituisce, come si è avuto modo di illustrare, una materia estremamente complessa per lo studioso del processo penale. Questi, infatti, si trova nella difficile posizione di dover trovare un raccordo tra le particolarità dell'informatica e gli istituti del processo penale. Al netto del gran numero di informazioni che possono essere reperibili grazie agli sviluppi della tecnologia e della scienza nel settore informatico, sembrerebbero, quasi di pari passo, aumentare per quantità e qualità i problemi di compatibilità tra gli strumenti resi disponibili da tali nuove conoscenze e il codice di rito penale.

Senza voler richiamare nella loro totalità le considerazioni precedentemente svolte, si può, tuttavia, a titolo esemplificativo fare riferimento alla tematica del sequestro di materiale informatico e a quella del captatore informatico[1]. La prima costituisce, come si è visto, un momento di scontro tra le esigenze tecniche e la garanzia dei diritti dei singoli. Infatti seguendo le *best practises*, sembrerebbe necessario che l'acquisizione al processo penale di un *hard disk* debba avvenire grazie allo strumento della *bitstream image*, ossia attraverso la riproduzione integrale dello stesso. Tuttavia tale ipotesi pone più di un problema per quanto riguarda sia la tutela del diritto alla riservatezza di chi subisce la duplicazione del supporto e sia la compatibilità col principio di proporzionalità. Dal canto suo, il captatore informatico se costituisce, da un lato, una importante risorsa per gli inquirenti, dall'altro lato, pone in estremo pericolo beni giuridici di fondamentale importanza.

[1] Più in generale sul tema del sequestro di dati informatici si rimanda alle considerazioni svolte nel Cap. IV, § 2; sul captatore informatico, v. Cap. V, §§ 1 – 3.

In questo quadro si può innanzitutto sottolineare come l'approccio frammentario prescelto dal legislatore, forse giustificabile in passato, non appaia ormai più soddisfacente[2]. Infatti la mancanza, allo stato, di un *corpus* normativo omogeneo e idoneo a regolare l'ingresso nel processo penale dei dati informatici genera numerose questioni di difficile soluzione. Di conseguenza la strada da intraprendere passa necessariamente attraverso un nuovo intervento legislativo, con cui si affronti il tema della prova informatica in tutta la sua latitudine, approntando i necessari correttivi al codice di procedura penale.

Volendo tracciare una linea da seguire per un eventuale provvedimento legislativo, si deve sottolineare come il punto di partenza di qualsiasi approccio alla prova informatica non possa che essere rappresentato dalla necessità di offrire un bilanciamento tra i diversi interessi, spesso contrapposti, che vengono in gioco allorché debbano essere utilizzate tecniche di *digital forensics*. Queste posizioni giuridiche soggettive, oggetto di un sistema multilivello di garanzie spaziano dal diritto alla riservatezza, a quello dell'inviolabilità del domicilio e, infine, in quello alla libertà e segretezza delle comunicazioni.

In tale ottica deve essere sicuramente valorizzato lo schema fatto proprio sia dalla Costituzione sia dalle Carte dei diritti sovranazionali, le quali cercano di ricondurre ad armonia il sistema, ammettendo la momentanea compressione dei diritti del singolo soltanto se prevista dalla legge e disposta dal giudice. Non solo: sempre facendo riferimento ai princìpi cui dovrebbe ispirarsi un eventuale intervento novellistico, deve, quantomeno, farsi un accenno al canone della neutralità tecnica, il quale trova riscontro nel diritto dell'Unione europea. La recentissima direttiva 2016/680/UE, in tema di protezione dei dati personali, espressamente afferma che «la protezione delle persone fisiche dovrebbe essere neutrale

[2] Ci si riferisce sostanzialmente alla l. 18 marzo 2008, n. 48 di ratifica della Convenzione di Budapest sul *cybercime* di cui si è discusso principalmente nel Cap. IV.

sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate». In sostanza il nucleo fondamentale di tale principio sarebbe costituito dall'idea per cui l'attenzione del legislatore non debba concentrarsi tanto sugli strumenti tecnici utilizzabili nelle indagini penali, quanto semmai sulle modalità di protezione dei diritti che potrebbero essere compressi dall'attività inquirente.

Tale canone è, forse, in grado di cogliere quella che è la particolarità maggiore delle evidenze di carattere informatico, ossia la loro costante e rapida evoluzione. Sotto questo profilo il compito affidato al legislatore non appare affatto leggero. Un intervento eccessivamente specifico rischierebbe di essere inutile in un'ottica di medio-lungo periodo.

Partendo da tale considerazione, e scendendo più nello specifico, sono apprezzabili quelle proposte avanzate da chi ritiene necessario creare un istituto ibrido, il quale ponga al centro non tanto il mezzo di ricerca della prova da utilizzare quanto i diritti fondamentali che potrebbero da questo essere lesi[3]. In tale prospettiva la richiesta autorizzativa al giudice da parte del pubblico ministero sarebbe necessaria tutte le volte in cui l'acquisizione al procedimento di dati informatici debba avvenire attraverso una compressione del diritto alla *privacy*, inteso anche sotto il profilo della riservatezza informatica[4]. Il pregio di una tale soluzione sarebbe costituito dalla sua flessibilità: anche il metodo più innovativo potrebbe rientrare in tale ampia fattispecie. Più concretamente, la principale fonte di ispirazione per una tale normativa potrebbe essere rappresentata dalla disciplina delle intercettazioni. Per cui, il legislatore dovrebbe individuare da un lato, quelli che sono i reati per i quali sia ammesso

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

[4] Tema discusso nel Cap. III, § 3.

l'uso di strumenti di indagine informatica e, dall'altro, i presupposti per ottenere il provvedimento autorizzativo. Inoltre, sempre nell'ottica di effettuare un corretto bilanciamento tra l'esigenza di riservatezza del singolo e quella di repressione dei reati, si potrebbe prevedere un momento di *discovery* successivo allo svolgimento delle operazioni, tutte le volte in cui queste debbano essere compiute in segreto.

Si è consci, tuttavia, del fatto che, in attesa di un auspicabile intervento legislativo, sia la magistratura ad essere chiamata ad elaborare le soluzioni più opportune per tutti i problemi generati dalla prassi investigativa quotidiana. In relazione a tale aspetto si può sottolineare come, da un lato, la nostra Costituzione e le Carte dei diritti europee offrano sicuri appigli per un'interpretazione delle disposizioni codicistiche che sia il più possibile orientata alla tutela dei diritti dei singoli e, dall'altro, come la giurisprudenza di legittimità abbia ormai raggiunto una certa consapevolezza circa l'importanza delle questioni poste dall'impiego degli strumenti di *digital forensics* all'interno del procedimento penale.

Sul punto, a mero titolo di esempio, appaiono sicuramente interessanti e degni di nota alcune recenti asserzioni della Corte di cassazione in tema di sequestro di *hard disk* e di diritto al riesame del medesimo provvedimento[5]. In tali pronunce, come si è in precedenza cercato di illustrare i giudici del Supremo collegio hanno dimostrato una certa attenzione per quanto riguarda le peculiarità del dato informatico in relazione al problema della copia e duplicazione dello stesso. Al riguardo, si è riconosciuto come il dato informatico, caratterizzandosi per la riproducibilità globale, l'indistinguibilità della riproduzione, la sostanziale indifferenza del supporto, rispetto al dato originale renda irrilevante la diversità concettuale tra il dato riprodotto ed il suo originale. Conseguenza di tale impostazione è stata quella di

[5] Cfr. Cass. sez. VI, 24 febbraio 2015, Rizzo, in *C.e.d. cass.* n. 264092 e Cass. sez. III, 23 giugno 2015, Cellino, in *C.e.d. cass.* n. 265181, illustrate nel Cap. IV, § 3.

riconoscere la sussistenza di un interesse al riesame del provvedimento di sequestro anche qualora il supporto oggetto del provvedimento ablativo sia stato restituito.

Non solo: anche la sentenza delle Sezioni Unite in tema di captatore informatico si segnala, pur con i limiti individuati dai primi commentatori, per la volontà di ricercare, pur all'interno delle coordinate normative del codice di rito penale, un buon compromesso tra le esigenze investigative e quelle di tutela dei diritti dei singoli.

Bibliografia

- Aa. Vv., Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, a cura di L. Lupária, Giuffrè, Milano, 2012
- Aa. Vv., *Sistema penale e criminalità informatica*, a cura di L. Lupária, Giuffrè, Milano, 2008
- ABBAGNALE, M. T., *In tema di captatore informatico*, in *Arch. pen. web*, 2016, n. 2, pp. 1 ss.
- ALCARO, F., *Riflessioni "vecchie" e "nuove" in tema di beni immateriali. Il diritto d'autore nell'era digitale*, in *Rass. dir. civ.*, 2006, pp. 899 ss.
- ALESSI, G., *Il processo penale. Profilo storico*, Laterza, Bari, 2001
- ALMA, M. – PERRONI, C., *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Dir. pen. proc.*, 1997, pp. 504 ss.
- AMATO, G., sub *art. 14*, in *Commentario della Costituzione. Rapporti civili*, a cura di G. Branca, Zanichelli, Bologna, 1977, pp. 54 ss.
- AMODIO, E., *Dal sequestro in funzione probatoria al sequestro preventivo: nuove dimensioni della «coercizione reale» nella prassi e nella giurisprudenza*, in *Cass. pen.*, 1982, pp. 1073 ss.
- AMORTH, A., *La Costituzione italiana. Commento sistematico*, Giuffrè, Milano, 1948
- APRATI, R., *Le prove contraddittorie:* id est *il diritto al contraddittorio sul medesimo tema probatorio*, in *Dir. pen. proc.*, 2006, pp. 627 ss.
- APRILE, E., *Le indagini tecnico-scientifiche: problematiche giuridiche sulla formazione della prova penale*, in *Cass. pen.*, 2003, pp. 4043 ss.
- ATERNO, S., *La* computer forensics *tra teoria e prassi: elaborazioni dottrinali e strategie processuali*, in *Ciberspazio e diritto*, 2006, pp. 425 ss.
- ATERNO, S., *Art. 8*, in Cybercrime, *responsabilità degli enti e prova digitale*, a cura di G. Corasanniti – G. Corrias Lucente, Cedam, Padova, 2009, pp. 193 ss.
- ATERNO, S., Digital forensics *(investigazioni informatiche)*, in *Dig. pen.*, Utet, Torino, 2014, agg. VIII, pp. 217 ss.

- ATERNO, S., *L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nella* privacy, in *Arch. pen. web*, 2016, n. 1, pp. 1 ss.
- BALDASSARRE, A., Privacy *e costituzione: l'esperienza statunitense*, Bulzoni, Roma, 1967
- BALDUCCI, P., *Perquisizione (diritto processuale penale*, in *Enc. dir.*, Giuffrè, Milano, 2000, agg. IV, pp. 979 ss.
- BALDUCCI, P., *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria*, Giuffrè, Milano, 2002
- BALSAMO, A., *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen.*, 2016, pp. 2274 ss.
- BARBERA, A., sub *art. 2*, in *Commentario alla costituzione. Princìpi fondamentali*, a cura di G. Branca, Zanichelli, Bologna, 1975, pp. 50 ss.
- BARGIS, M., *Perquisizione*, in *Dig. pen.*, Utet, Torino, 1995, pp. 488 ss.
- BARGIS, M., *Note in tema di prova scientifica nel processo penale*, in *Riv. dir. proc.*, 2011, pp. 47 ss.
- BARILE, P. – CHELI, E., *Domicilio (libertà di)*, in *Enc. dir.*, Giuffrè, Milano, 1962, vol. XIII, pp. 859 ss.
- BARILE, P. –CHELI, E., *Corrispondenza (libertà di)*, in *Enc. dir.*, Giuffrè, Milano, 1962, vol. X, pp. 743 ss.
- BARILE, P., *Le libertà nella Costituzione. Lezioni*, Cedam, Padova, 1966
- BARILE, P., *Diritti dell'uomo e libertà fondamentali*, il Mulino, Bologna, 1984
- BARILI, P., *Accertamenti informatici*, in *Le indagini scientifiche nel procedimento penale*, a cura di R.V.O. Valli, Giuffrè, Milano, 2013, pp. 589 ss.
- BELLORA, P., *Ispezione giudiziale*, in *Dig. pen.*, Utet, Torino, 1993, vol. VII, pp. 275 ss.
- BELLUTA, H., *Imparzialità del giudice e dinamiche probatorie* ex officio, Giappichelli, Torino, 2006
- BENE, T., *Trasnazionalità dei crimini nella società confessionale: i pericoli della tecnologia e del diritto*, in *Giur. it.*, 2016, pp. 717 ss.
- BERGHELLA, F. –BLAIOTTA, R., *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, pp. 2329 ss.
- BIGNAMI, M., *Le gemelle crescono in salute: la confisca urbanistica tra Costituzione, C.e.d.u., e diritto vivente*, in *Dir. pen. cont.*, 2015, n. 2., pp. 288 ss.

- BOUCHARD, M., *Art. 134*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. II, pp. 147 ss.
- BRAGHÒ, G., *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa*, in *Dir. inf.*, 2005, pp. 517 ss.
- BRICOLA, F., *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. dir. proc. pen.*, 1967, pp. 1079 ss.
- BRUSCO, C., *Il vizio di motivazione nella valutazione della prova scientifica*, in *Dir. pen. proc.*, 2004, pp. 1412 ss.
- BRUSCO, C., *La valutazione della prova scientifica*, in *La prova scientifica nel processo penale*, a cura di P. Tonini, Ipsoa, Milano, 2008, pp. 23 ss.
- BRUSCO, C., *Scienza e processo penale: brevi appunti sulla valutazione della prova scientifica*, in *Riv. it med. leg.*, 2012, pp. 61 ss.
- BUONOMO, G., *Metodologia e disciplina delle indagini informatiche*, in R. Borruso – G. Buonomo – G. Corasaniti – G. D'Aietti, *Profili penali dell'informatica*, Giuffrè, Milano, 1994, pp. 135 ss.
- CACCAVELLA, D., *Gli accertamenti tecnici in ambito informatico e telematico*, in S. Aterno – P. Mazzotta, *La perizia e la consulenza tecnica*, Cedam, Padova, 2006, pp. 195 ss.
- CAIANIELLO, M., *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont.*, 2014, nn. 3-4, pp. 143 ss.
- CAJANI, F., *Il vaglio dibattimentale della* digital evidence, in *Arch. pen.*, 2013, pp. 837 ss.
- CALAMANDREI, I., *La prova documentale*, Cedam, Padova, 1995
- CAMON, A., *Le intercettazioni nel processo penale*, Giuffrè, Milano, 1996 CAMON, A., *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005, pp. 594 ss.
- CANTONE, R., *Perquisizioni e sequestri: dalle tecniche investigative alle problematiche processuali*, in *Arch. n. proc. pen.*, 2001, pp. 3 ss.
- CANZIO, G., *Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale*, in *Dir. pen. proc.*, 2003, pp. 1193 ss.
- CANZIO, G., *Prova scientifica, ricerca della "verità" e decisione giudiziaria nel processo penale*, in Aa. Vv., *Decisione giudiziaria e verità scientifica*, Giuffrè, Milano, 2005, pp. 55 ss.

- CAPITANI, S., *Brevi considerazioni sulla* Bloodstain pattern analysis *nel procedimento penale*, in *Dir. pen. proc.*, 2015, pp. 487 ss.
- CAPRIOLI, F., *Colloqui riservati e prova penale*, Giappichelli, Torino, 2000
- CAPRIOLI, F., *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, pp. 3520 ss.
- CAPRIOLI, F., Scientific evidence *e logiche del probabile nel processo per il "delitto di Cogne"*, in *Cass. pen.*, 2009, pp. 1867 ss.
- CARETTI, P., *Domicilio (libertà di)*, in *Dig. discl. pubbl.*, Giuffrè, Milano, 1990, vol. V, pp. 320 ss.
- CARLI, V. L., *Le indagini preliminari nel sistema processuale penale: accusa e difesa nella ricerca e predisposizione della prova penale*, Giuffrè, Milano, 2° ed., 2005
- CARNELUTTI, F., *Documento (teoria moderna)*, in *Novissimo dig. it.*, Utet, Torino, 1960, vol. VI, pp. 85 ss.
- CARNEVALE, S., *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in *Protezione dei dati personali e accertamento penale*, a cura di D. Negri, Aracne, Roma, 2007, pp. 3 ss.
- CARNEVALE, S., *I rimedi contro il giudicato tra vizi procedurali e "vizi normativi"*, in *All'incrocio tra Costituzione e Cedu. Il ragno delle norme della Convenzione e l'efficacia interna delle sentenze di Strasburgo*, a cura di R. Bin – G. Brunelli – A. Pugiotto – P. Veronesi, Giappichelli, Torino, 2007, pp. 57 ss.
- CARNEVALE, S., *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. proc.*, 2009, pp. 469 ss.
- CARRARA, F., *Programma del corso di diritto criminale. Parte generale*, Giusti, Lucca, 6° ed., 1886
- CARTABIA, M., *Le sentenze «gemelle»: diritti fondamentali, fonti, giudici*, in *Giur. cost.*, 2007, pp. 3565 ss.
- CARTABIA, M., *La convenzione europea dei diritti dell'uomo e l'ordinamento italiano*, in *Giurisprudenza europea e processo penale italiano. Nuovi scenari dopo il «caso Dorigo» e gli interventi della Corte costituzionale*, a cura di A. Balsamo – R. E. Kostoris, Giappichelli, Torino, 2008, pp. 33 ss.

- CASASOLE, F., *Neuroscienze, genetica comportamentale e processo penale*, in *Dir. pen. proc.*, 2012, pp. 110 ss.
- CASEY, E., *Digital evidence and computer crime. Forensic science, computer and the internet*, Academic Press, Cambridge, Massahussets, 3° ed., 2011
- CASSIBBA, F., *Investigazioni ed indagini preliminari*, in *Dig. pen.*, Utet, Torino, 2004, agg. II, pp. 509 ss.
- CATAUDELLA, A., *Riservatezza (diritto alla) I) diritto Civile*, in *Enc. giur. Treccani*, Roma, 1994, pp. 1 ss.
- CERQUA, F., *Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche*, in *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 marzo 2008, n. 48)*, a cura di L. Lupária, Giuffrè, Milano, 2009, pp. 221 ss.
- CERQUA, F., *Ancora dubbi e incertezze sull'acquisizione della corrispondenza elettronica*, in *www.penalecontemporaneo.it*, pp. 1 ss.
- CHELO MANCHÌA, A., *Sequestro probatorio di* computers*: un provvedimento superato dalla tecnologia?*, in *Cass. pen.*, 2005, pp. 1634 ss.
- CHIARELLI, R., *Domicilio I) libertà di domicilio*, in *Enc. giur. Treccani*, Roma, 1989, pp. 1 ss.
- CHIAVARIO, M., *Considerazioni sul diritto alla prova nel processo penale*, in *Cass. pen.*, 1996, pp. 2009 ss.
- CHIAVARIO, M., *Art. 6*, in *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, a cura di S. Bartole – B. Conforti – G. Raimondi, Cedam, Padova, 2001, pp. 154 ss.
- CHIAVARIO, M., *Giusto processo II) processo penale*, in *Enc. giur. Treccani*, Roma, 2001, pp. 1 ss.
- CISTERNA, A., *Perquisizioni in caso di fondato motivo*, in *Guida dir.*, 2008, f. 16, pp. 59 ss.
- CISTERNA, A., *All'Aise l'attività d'informazione verso l'estero*, in *Guida dir.*, 2015, f. 19, pp. 94 ss.
- CISTERNA, A., *Cedu e diritto alla privacy*, in *I princìpi europei del processo penale*, a cura di A. Gaito, Dike giuridica editrice, Roma, 2016, pp. 193 ss.

- COLAIOCCO, S., *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. pen. web*, 2014, n. 1, pp. 1 ss.
- COLOMBO, E., *La sentenza del caso di Garlasco e la* computer forensics*: analisi di un complesso rapporto tra diritto ed informatica*, in *Cyberspazio e diritto*, 2010, pp. 447 ss.
- COLOMBO, E., *"*Data Retention*" e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen.*, 2014, pp. 2705 ss.
- COMOGLIO, L.P., *Prove ed accertamento dei fatti nel nuovo c.p.p.*, in *Riv. it. dir. proc. pen.*, 1990, pp. 113 ss.
- CONSO, G., *Natura giuridica delle norme sulla prova nel processo penale*, in *Riv. dir. proc.*, 1970, pp. 7 ss.
- COSTANZO, P., *La dimensione costituzionale della* privacy, in *La legge sulla* privacy *dieci anni dopo*, a cura di G. F. Ferrari, Egea, Milano, 2008, pp. 49 ss.
- CONTI, C., *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, Padova, 2007
- CONTI, C., *L'attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, in *Le nuove norme sulla sicurezza pubblica*, a cura di S. Lorusso, Cedam, Padova, 2008, pp. 3 ss.
- CONTI, C., Iudex peritus peritorum *e ruolo degli esperti nel processo penale*, in *La prova scientifica nel processo penale*, a cura di P. Tonini, Ipsoa, Milano, 2008, pp. 29 ss.
- CONTI, C., *Intercettazioni e inutilizzabilità: la giurisprudenza aspira al sistema*, in *Cass. pen.*, 2011, pp. 3638 ss.
- CONTI, C., *La prova scientifica*, in *La prova penale*, a cura di P. Ferrua – E. Marzaduri – G. Spangher, Giappichelli, Torino, 2013, pp. 87 ss.
- CONTI, G., *Forme di documentazione, forme di verbalizzazione e strumenti di documentazione: alcune precisazioni a margine di una sentenza della Corte costituzionale*, in *Cass. pen.*, 1991, II, pp. 90 ss.
- CORASANITI, G., *Prove digitali e interventi giudiziari sulla rete nel percorso della giurisprudenza di legittimità*, in *Dir. inf.*, 2011, pp. 399 ss.
- CORDERO, F., *Procedura penale*, Giuffrè, Milano, 9° ed., 2012
- CORDÌ, L., *Commento all'art. 8 l. 18 marzo 2008, n. 48*, in *Leg. pen.*, 2008, pp. 280 ss.

- COSSIGNANI, M., *Il contributo tecnico nel processo: la novità della consulenza* extra perita, in *Dir. pen. proc.*, 1997, pp. 333 ss.
- COSTABILE, G., Scena criminis, *documento informatico e formazione della prova*, in *Dir. inf.*, 2005, pp. 53 ss.
- COSTABILE, G., Computer forensic *e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Ciberspazio e diritto*, 2010, pp. 465 ss.
- COSTANZO, P., *La dimensione costituzionale della* privacy, in G.F. Ferrari, *La legge sulla* privacy *dieci anni dopo*, Egea, Milano, 2008, pp. 49 ss.
- CUOMO, L., *La tutela penale del domicilio informatico*, in *Cass. pen.*, 2000, pp. 2990 ss.
- CURTOTTI NAPPI, D. – SARAVO, L., *Sopralluogo giudiziario*, in *Dig. pen.*, Utet, Torino, 2011, agg. VI, pp. 587 ss.
- CURTOTTI, D., *Rilievi e accertamenti*, Cedam, Padova, 2013
- D'AMBROSIO, L. – VIGNA, P. L., *La pratica di polizia giudiziaria*, Cedam, Padova, 6° ed., 2006
- D'AMBROSIO, L., *La polizia giudiziaria nel processo penale*, in L. D'Ambrosio, *La pratica di polizia giudiziaria*, Cedam, Padova, 7° ed., 2007, vol. I
- DANIELE, M., *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, pp. 283 ss.
- DANIELE, M., *La formazione digitale delle prove dichiarative. L'esame a distanza tra regole interne e diritto sovranazionale*, Giappichelli, Torino, 2012
- DANIELE, M., *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, pp. 441 ss.
- DANIELE, M., *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?* in *Cass. pen.*, 2013, pp. 367 ss.
- DANIELE, M., *Norme processuali convenzionali e margine di apprezzamento nazionale*, in *Cass. pen.*, 2015, pp. 1690 ss.
- DE CRESCIENZO, U., *Il sequestro penale e civile*, Utet, Torino, 1997
- DE FLAMMINEIS, S., *Le intercettazioni telematiche*, in *Dir. pen. proc.*, 2013, 988 ss.
- DE LEO, F., *Le indagini tecniche di polizia. Un invito al legislatore*, in *Cass. pen.*, 1996, pp. 697 ss.
- DE LUCA, G., *Il sistema delle prove penali e il principio del libero convincimento nel nuovo rito*, in *Riv. it. dir. proc. pen.*, 1992, pp. 1255 ss.

- DE LUCA, G., *Profilo storico del libero convincimento del giudice*, in Aa. Vv., *Il principio del libero convincimento del giudice nel nuovo processo penale*, in *Quad. C.S.M.*, 1992, pp. 9 ss.
- DE RUGERIIS, G., *Effetti delle innovazioni tecnologiche sul processo penale*, in *Questioni di informatica forense*, a cura di C. Maioli, Aracne, Roma, 2015, pp. 89 ss.
- DE SÁ, P. – LEONOR CHASTRE, C., *L'utilizzo del captatore informatico "Trojan Horse" nella procedura penale portoghese*, in *Parola alla difesa*, 2016, pp. 183 ss.
- DE SANTIS, A. M., *Sequestro preventivo*, in *Dig. pen.*, Utet, Torino, 1997, vol. XIII, pp. 264 ss.
- DEL POZZO, C. U., *Corpo del reato* in *Enc. dir.*, Giuffrè, Milano, 1962, vol. X, pp. 650 ss.
- DELLA MORTE, M., *Art. 14*, in *Commentario alla Costituzione*, a cura di R. Bifulco – A. Celotto – M. Olivetti, Utet, Torino, 2006, pp. 342 ss.
- DENTI, V., *Scientificità della prova e libera valutazione del giudice*, in *Riv. dir. proc.*, 1972, pp. 414 ss.
- DI PAOLO, G., *Le novità del Parlamento Europeo e Consiglio – direttiva del 15 marzo 2006, 2006/24/CE, riguardante la conservazione dei dati generati e trattati nell'ambito della fornitura dei servizi accessibili al pubblico di comunicazione elettronica e di reti pubbliche di comunicazione che modifica la direttiva 2002/58/CE*, in *Cass. pen.*, 2006, pp. 2196 ss.
- DI PAOLO, G., *Acquisizione dinamica dei dati relativi all'ubicazione del cellulare ed altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense*, in *Cass. pen.*, 2008, pp. 1219 ss.
- DI PAOLO, G., *Prova informatica (diritto processuale)*, in *Enc. dir.*, Giuffrè, Milano, 2013, ann. VI, pp. 736 ss.
- DOMINIONI, O., *In tema di nuova prova scientifica*, in *Dir. pen. proc.*, 2001, pp. 1061 ss.
- DOMINIONI, O., *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005DOMINIONI, O., *L'ammissione della nuova prova penale scientifica*, in *La prova scientifica nel processo penale*, a cura di P. Tonini, Ipsoa, Milano, 2008, pp. 21 ss.
- DOMINIONI, O., *Prova scientifica (diritto processuale penale)*, in *Enc. dir.*, Giuffrè, Milano, 2008, ann. II, t. I, pp. 976 ss.

- DOMINIONI, O., *L'esperienza italiana di impiego della prova scientifica nel processo penale*, in *Dir. pen. proc.*, 2015, pp. 601 ss.
- DONDI, A., *Paradigmi processuali ed* "expert testimony" *nel diritto statunitense*, in *Riv. trim. dir. proc. civ.*, 1996, pp. 261 ss.
- DONDI, A., *Problemi di utilizzazione delle «conoscenze esperte» come «*expert witness testimony*» nell'ordinamento statunitense*, in *Riv. trim. proc. civ.*, 2001, pp. 1133 ss.
- ESPOSITO, E., *Prova scientifica*, in *Dig. pen.*, Utet, Torino, 2005, agg. III, pp. 1230 ss.
- ESTER RICCI, A., Digital evidence *e irriperibilità delle operazioni acquisitive*, in *Dir. pen. proc.*, 2010, pp. 337 ss.
- FAIGMAN, DAVID L.; KAYE, DAVID H.; SAKS, MICHAEL J. & SANDERS, JOSEPH, *Modern Scientific Evidence: The Law and Science of Expert Testimony, Admissibility of scientific evidence: The general Acceptance Standard of Frye*, St. Paul, Minn.: West Publishing co., 2° ed., 2002
- FALATO, F., *Sulla categoria dei mezzi atipici di ricerca della prova e le c.d. intercettazioni Gps*, in *Giur. it.*, 2010, pp. 11 ss.
- FANCHIOTTI, V., *Il cyberorecchio di dionisio*, in *Cass. pen.*, 2015, pp. 1645 ss.
- FASO, I., *La libertà di domicilio*, Giuffrè, Milano, 1968
- FASOLIN, S., *La copia di dati informatici nel quadro delle categorie processuali*, in *Dir. pen. proc.*, 2012, pp. 372 ss.
- FASSONE, E., *Dalla "certezza" all'"ipotesi preferibile": un metodo per la valutazione*, in *Riv. it. dir. proc. pen.*, 1995, pp. 1104 ss.
- FEDERICI, C., *Nuovi orizzonti per l'acquisizione remota di* Personal Cloud Storage, in *Questioni di informatica forense*, a cura di C. Maioli, Aracne, Roma, 2015, pp. 113 ss.
- FELICIONI, P., *Le ispezioni e perquisizioni*, Giuffrè, Milano, 2° ed., 2012
- FELICIONI, P., *Prova scientifica*, in *Dig. pen.*, Utet, Torino, 2014, agg. VIII, pp. 611 ss.
- FELICIONI, P., *L'acquisizione di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. giust.*, 2016, n. 5, pp. 118 ss.
- FERRAIOLI, M., *Misure cautelari*, in *Enc. giur. Treccani*, 1990, pp. 1 ss.
- FERRARI, F., *Il codice dell'amministrazione digitale e le norme dedicate al documento informatico*, in *Riv. dir. proc.*, 2007, pp. 415 ss.

- FERRUA, P., *Sulla legittimità della ricognizione compiuta contro la volontà dell'imputato*, in *Cass. pen.*, 1990, I, pp. 652 ss.
- FERRUA, P., *Metodo scientifico e processo penale*, in *La prova scientifica nel processo penale*, a cura di P. Tonini, Ipsoa, Milano, 2008, pp. 12 ss.
- FERRUA, P., *Il contraddittorio nella formazione della prova a dieci anni dalla sua costituzionalizzazione: il progressivo assestamento della regola e le insidie della giurisprudenza della Corte europea*, in *Arch. pen.*, 2008, n. 3, pp. 9 ss.
- FERRUA, P., *Il giudizio penale: fatto e valore giuridico*, in P. Ferrua – F.M. Griffantini – G. Illuminati – R. Orlandi, *La prova nel dibattimento penale*, Giappichelli, Torino, 4° ed., 2010, pp. 317 ss.
- FERRUA, P., *L'interpretazione della Convenzione europea dei diritti dell'uomo e il preteso monopolio della Corte di Strasburgo*, in *Proc. pen. giust.*, 2011, n. 4, pp. 116 ss.
- FILIPPI, L., *L'intercettazione di comunicazioni*, Giuffrè, Milano, 1997
- FILIPPI, L., *Il captatore informatico: l'intercettazione* ubicumque *al vaglio delle Sezioni Unite*, in *Arch pen. web*, 2016, n. 1, pp. 1 ss.
- FILIPPI, L., *L'ispe-perqui-intercettazione "itinerante": le Sezioni Unite azzeccano la diagnosi, ma sbagliano la terapia*, in *Parola alla difesa*, 2016, pp. 179 ss.
- FILIPPI, L., *Questioni nuove in tema di intercettazioni:* quid iuris *sul "*pin to pin*" dei* BlackBerry*?* in *Arch. pen. web*, 2016, n. 1, pp. 155 ss.
- FLOR, R., *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di "domicilio informatico" e lo* jus exludendi alios, in *Dir. pen. proc.*, 2005, pp. 81 ss.
- FLOR, R., *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgeright *sulla c.d.* online durchsuchung, in *Riv. trim. dir. pen. econ.*, 2009, pp. 695 ss.
- 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?*, in *Dir. pen. cont.*, 2014, n. 2, pp. 178 ss.
- FOCARDI, F., *La consulenza tecnica extraperitale delle parti private*, Cedam, Padova, 2003
- FOCARDI, F., *Art. 243*, in *Codice di procedura penale commentato*, a cura di A. Giarda – G. Spangher, Ipsoa, Milano, 4° ed., 2010, pp. 2413 ss.
- FRONZONI, V., *Perquisizioni*, in *Enc. giur. Treccani*, 2007, pp. 1 ss.

- FUMU, G., *Art. 266*, in *Commento al codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. II, pp. 771 ss.
- FUMU, G., *Art. 266* bis, in *Commento al codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1997, agg. III, pp. 129 ss.
- FÙRFARO, S., *Il diritto alla riservatezza,* in *Riservatezza ed intercettazioni tra norma e prassi*, a cura di A. Gaito, Aracne, Roma, 2011, pp. 21 ss.
- FÙRFARO, S., *Le intercettazioni "*pin to pin*" del sistema* BlackBerry*, ovvero: quando il vizio di informazione tecnica porta a conclusioni equivoche*, in *Arch. pen. web*, 2016, n. 1, pp. 1 ss.
- GAITO, A. – FÙRFARO, S., *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, in *I princìpi europei del processo penale*, a cura di A. Gaito, Dike giuridica editrice, Roma, 2016, pp. 363 ss.
- GAITO, A. –FÙRFARO, S., *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen. web*, 2016, n. 2, pp. 1 ss.
- GALDIERI, P., *La tutela penale del domicilio informatico*, in *Problemi giuridici dell'informatica nel MEC*, a cura di P. Galdieri, Giuffrè, Milano, 1996, pp. 189 ss.
- GALLUCCIO, A., *Profili generali sugli art. 8-11*, in *Corte di Strasburgo e giustizia penale*, a cura di G. Ubertis – F. Viganò, Giappichelli, Torino, 2016, pp. 255 ss.
- GENNARI, G., *Scienziati e giudici: l'incontro (im)possile*, in *Medicina e diritto*, 2010, f. 3, pp. 7 ss.
- GENTILE, D., Tracking *satellitare mediante gps: attività atipica di indagine o intercettazione di dati?*, in *Dir. pen. proc.*, 2010, pp. 1464 ss.
- GENTILI, A., *Documento informatico (diritto civile)*, in *Enc. dir.*, Giuffrè, Milano, 2012, ann. V, pp. 629 ss.
- GHIRARDINI, A – FAGGIOLI, G., Digital forensics, Apogeo, Milano, 3° ed., 2013
- GIAMBRUNO, S., *Polizia giudiziaria*, in *Dig. pen.*, Utet, Torino, 1995, vol. IX, pp. 597 ss.
- GIANFROTTA, F., *Art. 220*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. II, pp. 571 ss.

- GIANNITI, P., *La «comunitarizzazione» della «carta» a seguito del trattato di Lisbona*, in *I diritti fondamentali nell'Unione europea. La Carta di Nizza dopo il Trattato di Lisbona*, a cura di P. Gianniti, Zanichelli, Bologna, 2012, pp. 357 ss.
- GIORDANO, L. – VENEGONI, A., *La corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *www.penalecontemporaneo.it*
- GIOSTRA, G., *Contraddittorio (principio del) II) diritto processuale penale*, in *Enc. giur. Treccani*, Roma, 2001, pp. 1 ss.
- GIUNCHEDI, F., *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, Utet, Torino, 2009, pp. 23 ss.
- GIUNCHEDI, F., *Accertamenti tecnici*, in *Dig. pen.*, Utet, Torino, 2010, agg. V, pp. 1 ss.
- GIUNCHEDI, F., *Le* malpractices *della* digital forensics. *Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *Arch. pen.*, 2013, pp. 821 ss.
- GRAZIOSI, A., *Documento informatico (diritto processuale civile)*, in *Enc. dir.*, Giuffrè, Milano, 2008, ann. II, pp. 491 ss.
- GREVI, V., Nemo tenetur se detegere*: interrogario dell'imputato e diritto al silenzio nel processo penale italiano*, Giuffrè, Milano, 1972
- GREVI, V., *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche* in *Giur. cost.*, 1973, pp. 317 ss.
- GREVI, V., *Un'occasione perduta (o forse solo rinviata) dalla Corte costituzionale in tema di uso distorto della richiesta di rimessione del processo*, in *Cass. pen.*, 1996, pp. 451 ss.
- GREVI, V., *Prove*, in *Compendio di procedura penale*, a cura di G. Conso, V. Grevi, M. Bargis, Cedam, Padova, 8° ed., 2015, pp. 281 ss.
- GRIFFANTINI, F. M., *Riesame del sequestro e valutazione dei presupposti nella giurisprudenza sul c.p.p. 1930 e nel c.p.p. del 1988* in *Riv. it. dir. proc. pen.*, 1990, pp. 164 ss.
- GRILLO, A. – MOSCATO, U.E., *Riflessioni sulla prova informatica*, in *Cass. pen.*, 2010, pp. 372 ss.
- GROSSI, P., *Inviolabilità dei diritti*, in *Enc. dir.*, Giuffrè, Milano, 1972, vol. XXIII, pp. 712 ss.
- GUALTIERI, P., *Diritto di difesa e prova scientifica*, in *Dir. pen. proc.*, 2011, pp. 493 ss.

- GUAZZAROTTI, A., *La Corte e la CEDU: il problematico confronto di* standard *di tutela alla luce dell'art. 117, comma 1, Cost*, in *Giur. cost.*, 2007, pp. 3574 ss.
- GUSPINI, U., *L'orecchio del regime: le intercettazioni telefoniche al tempo del fascismo*, Milano, Mursia, 1973
- HUBERT, P., *Galileo's Revenge: Junk Science in the Courtroom*, Basic books, New York, 1993
- HUTCHINSON, C.T. – ASHBY, D. S., *Daubert v. Merrell Dow Pharmaceuticals, Inc.: redefining the bases for admissibility of expert scientific testimony*, in *Cardozo L. Rev.*, 1994, pp. 1880 ss.
- IACOBACCI, D., *Sulla necessità di riformare la disciplina delle intercettazioni prendendo le mosse dalle esitazioni applicative già note*, in *Giust. pen.*, 2001, III, cc. 361 ss.
- IACOVIELLO, F., *La motivazione della sentenza penale e il suo controllo in cassazione*, Giuffrè, Milano, 1997
- ILLUMINATI, G., *La disciplina processuale delle intercettazioni*, Giuffrè, Milano, 1983
- IOVENE, F., *Perquisizione e sequestro di* computer*: un'analisi comparatistica*, in *Riv. dir. proc.*, 2012, pp. 1607 ss.
- IOVENE, F., Data retention *tra passato e futuro. Ma quale presente?*, in *Cass. pen.*, 2014, pp. 4274 ss.
- IOVENE, F., *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont.*, 2014, nn. 3-4, pp. 3295 ss.
- IRTI, N., *Norme e fatti. Saggi di teoria generale del diritto,* Giuffrè, Milano, 1984
- JESU, G., *Inaccettabili approdi in tema di sequestro probatorio*, in *Cass. pen.*, 1999, pp. 1078 ss.
- LA MUSCATELLA, D., *La genesi della prova digitale: analisi prospettica dell'ingresso dell'informatica forense nel processo penale*, in *Ciberspazio e diritto*, 2012, pp. 385 ss.
- LAMARQUE, E., *Le relazioni tra l'ordinamento nazionale, sovranazionale e internazionale nella tutela dei diritti*, in *Dir. pubbl.*, 2013, pp. 766 ss.
- LARONGA, A., *L'utilizzabilità probatoria del controllo a distanza eseguito con sistema satellitare g.p.s.*, in *Cass. pen.*, 2002, pp. 3050 ss.
- LASAGNI, G., *L'uso di captatori informatici (*trojans*) nelle intercettazioni "fra presenti"*, in *www.penalecontemporaneo.it*, pp. 1 ss.

- LE FÈVRE, P., *Il regime della captazione dei dati informatici nel diritto francese*, in *Parola alla difesa*, 2016, pp. 181 ss.
- LEONE, G., *Svolgimento del processo penale. Il processo di prima istanza*, in G. Leone, *Trattato di diritto processuale penale*, Jovene, Napoli, 1961, pp. 175 ss.
- LEOPIZZI, A., *La biblioteca (digitale) di Babele. Condotte umane nel cyberspazio e competenza territoriale per le violazioni del domicilio informatico*, in *Giust. pen.*, 2015, III, cc. 410 ss.
- LIGUORI, A., Extraordinary Redentions *nella giurisprudenza della Corte europea dei diritti umani: il caso Abu Omar*, in *Riv. dir. int.*, 2016, pp. 777 ss.
- LOGLI, A., *Sequestro probatorio di un* personal computer. *Misure* ad explorandum *e tutela della corrispondenza elettronica*, in *Cass. pen.*, 2008, pp. 2952 ss.
- LOMBARDO, L., *La scienza e il giudice nella ricostruzione del fatto*, in *Riv. dir. proc.*, 2007, pp. 35 ss.
- LORENZETTO, E., *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, pp. 1522 ss.
- LORUSSO, S., *La prova scientifica*, in *La prova penale*, diretto da A. Gaito, Utet, Torino, 2008, vol. I, pp. 295 ss.
- LUPÁRIA, L. – ZICCARDI, G., *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007
- LUPÁRIA, L., *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc.*, 2008, pp. 696 ss.
- LUPÁRIA, L., Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, diretto da G. Spangher, *Modelli differenziati di accertamento*, Utet, Torino, 2011, vol. VII, t. I, pp. 369 ss.
- MAFFEO, V., *Prova documentale II) diritto processuale penale*, in *Enc. giur. Treccani*, Roma, 1992, pp. 1 ss.
- MALINVERNI, A., *Teoria del falso documentale*, Giuffrè, Milano, 1958
- MANCUSO, E. M., *L'acquisizione di contenuti* e-mail, in *Le indagini atipiche*, a cura di A. Scalfati, Giappichelli, Torino, 2014, pp. 53 ss.
- MARAFIOTI, L., Digital evidence *e processo penale*, in *Cass. pen.*, 2011, pp. 4509

- MARCOLINI, S., *Le cosiddette perquisizioni* on line *(o perquisizioni elettroniche)*, in *Cass. pen.*, 2010, 2855 ss.
- MARCOLINI, S., *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015, pp. 760 ss.
- MARINELLI, C., *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, Torino, 2007
- MARINI, F. S., *La costituzionalità delle riprese visive nel domicilio: ispezione o libertà «sotto-ordinata»?*, in *Giur. cost.*, 2002, pp. 1076 ss.
- MARZADURI, E., *Azione*, *IV) diritto processuale penale*, in *Enc. giur. Treccani*, Roma, 1996, pp. 1 ss.
- MARZADURI, E., *Commento all'art. 1 l. cost. 23 novembre 1999, n. 2*, in *Leg. pen.*, 2000, pp. 762 ss.
- MASUCCI, A., *Il documento informatico. Profili ricostruttivi della nozione e della disciplina*, in *Riv. dir. civ.*, 2004, pp. 749 ss.
- MATTIUCCI, M. – DELFINIS, G., Forensic computing, in *Rass. arm. carabinieri*, 2006, pp. 51 ss.
- MAZZA, O., *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, Giuffré, Milano, 2004
- MELCHIONDA, A., *Sequestro (dir. proc. pen.)*, in *Enc. dir.*, Giuffrè, Milano, 1990, vol. XLII, pp. 148 ss.
- MELILLO, G., *Appunti in tema di sospensione feriale dei termini relativi a procedimenti per reati di criminalità organizzata*, in *Cass. pen.*, 2005, pp. 2925 ss.
- MINNECI, G. – ALIBRANDI, A. S., *Documento elettronico e telematico*, in *Dig. disc. priv.*, Utet, Torino, 2000, agg. I, pp. 342 ss.
- MOLINARI, F.M., *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2010, pp. 1259 ss.
- MOLINARI, F. M., *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2012, pp. 696 ss.
- MONTAGNA, M., *Sequestri*, in *Dig. pen.*, Utet, Torino, 2005, agg. III, pp. 1543 ss.

- MORELLI, F. B., *La giurisprudenza costituzionale italiana tra diritto alla riservatezza e potere di controllo sulle informazioni personali*, in *Protezione dei dati personali e accertamento penale*, a cura di D. Negri, Aracne, Roma, 2007, pp. 27 ss.
- MORELLI, F. B., *Videoriprese mediante la* webcam *di un computer illecitamente sottratto e tutela del domicilio*, in *Dir. pen. proc.*, 2013, pp. 475 ss.
- MOSCARINI, P., *Ispezione (diritto processuale penale)*, in *Enc. dir.*, Giuffrè, Milano, 1998, agg. II, pp. 464 ss.
- MOSCARINI, P., *Lo statuto della "prova scientifica" nel processo penale*, in *Dir. pen. proc*, 2015, pp. 649 ss.
- MOTZO, G., *Contenuto ed estensione della libertà domiciliare*, in *Rass. dir. pub.*, 1954, pp. 507 ss.
- MURGO, M., *Diritti di libertà*, in *I diritti fondamentali nell'Unione europea. La Carta di Nizza dopo il Trattato di Lisbona*, a cura di P. Gianniti, Zanichelli, Bologna, 2013, pp. 761 ss.
- MURGO, M., *Il diritto al rispetto della vita privata*, in *La CEDU e il ruolo delle Corti*, a cura di P. Gianniti, Zanichelli, Bologna, 2015, pp. 1155 ss.
- NAIKE CASCINI, D., *Messaggistica tra telefonia* Blackberry*: nuove prassi devianti al limite dell'abuso del processo*, in *Arch. pen. web*, 2016, n. 2, pp. 1 ss.
- NAPPI, A., *Guida al codice di procedura penale*, Giuffrè, Milano, 10° ed., 2007
- NAVONE, G., Instrumentum *digitale. Teoria e disciplina del documento informatico*, Giuffrè, Milano, 2012
- NOBILI, M., *Nuove polemiche sulle cosiddette «massime d'esperienza»*, in *Riv. it. dir. proc. pen.*, 1969, pp. 123 ss.
- NOBILI, M., *Art. 189*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. II, pp. 397 ss.
- NOBILI, M., *Art. 190*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. II, pp. 400 ss.
- NOBILI, M., *Art. 192*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. II, pp. 414 ss.
- NOBILI, M., *Libero convincimento del giudice*, in *Enc. giur. Treccani*, Roma, 1990, pp. 1 ss.

- NOCITA, P., *Consulente tecnico II) diritto processuale penale*, in *Enc. giur. Treccani*, 1988, pp. 1 ss.
- 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, pp. 1069 ss.
- NOVARIO, F., *Prove penali informatiche*, Edizioni libreria cortina, Torino, 2011
- NOVARIO, F., *Le prove informatiche*, in *La prova penale*, a cura di P. Ferrua – E. Marzaduri, G. Spangher, Giappichelli, Torino, 2013, pp. 121 ss.
- ORLANDI, R., *Atti e informazioni dell'autorità amministrativa nel processo penale. Contributo allo studio delle prove extrapenali*, Giuffrè, Milano, 1992
- ORLANDI, R., *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, pp. 129 ss.
- PACE, A., sub *art. 15* in *Commentario della Costituzione. Rapporti civili*, a cura di G. Branca, Zanichelli, Bologna, 1977, pp. 80 ss.
- PACE, A., *Problematica delle libertà costituzionali. Lezioni. Parte speciale*, Cedam, Padova, 2° ed., 1992
- PACE, A., *Metodi interpretativi e costituzionalismo*, in *Quaderni costituzionali*, 2001, f. 1, pp. 35 ss.
- PACE, A., *Le videoregistrazioni «ambientali» tra gli artt. 14 e 15 Cost.*, in *Giur. cost.*, 2002, pp. 1070 ss.
- PAGANETTO, G., *Le riprese visive nei luoghi di privata dimora. Spunti per una riflessione sui contenuti e i limiti della libertà di domicilio*, in *Forum di quaderni costituzionali on line*, 1 ss.
- PALMA, I., *Considerazione sul principio di tassatività dei mezzi di prova*, in *Riv. it. dir. proc. pen.*, 2009, pp. 400 ss.
- PAOLA, F. M., *Ricognizioni*, in *Dig. pen.*, Utet, Torino, 1997, vol. XII, pp. 218 ss.
- PARODI, C., *Il documento informatico nel sistema normativo penale*, in *Dir. pen. proc.*, 1998, pp. 369 ss.
- PARODI, C., *La disciplina delle intercettazioni telematiche*, in *Dir. pen. proc.*, 2003, pp. 889 ss.

- PARODI, C., VoIP, Skype *e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?* in *Dir. pen. proc.*, 2008, pp. 1309 ss.
- PATANÈ, V., *Il diritto al silenzio dell'imputato*, Giappichelli, Torino, 2006
- PAULESU, P. P., *Notizia di reato e scenari investigativi complessi: contrasto alla criminalità organizzata, operazioni «sotto copertura», captazione di dati digitali*, in *Riv. dir. proc.*, 2010, pp. 787 ss.
- PAZIENZA, F., *Domicilio IV) delitti contro la inviolabilità del domicilio*, in *Enc. giur. Treccani*, 1989, pp. 1 ss.
- PECORELLA, C., *Diritto penale dell'informatica*, Cedam, Padova, 2006
- PERETOLI, P., *Controllo satellitare con GPS: pedinamento o intercettazione?* in *Dir. pen. proc.*, 2003, pp. 93 ss.
- PERNA, F., *Il captatore informatico nell'attuale panorama investigativo: riflessi operativi*, in *Parola alla difesa*, 2016, pp. 170 ss.
- PERRI, P., Computer forensics *(indagini informatiche)*, in *Dig. pen.*, Utet, Torino, 2011, agg. VI, pp. 95 ss.
- PETRONE, M., *Le recenti modifiche del codice penale in tema di documento informatico: problemi e prospettive*, in *Dir. Inf.*, 1995, pp. 259 ss.
- PICA, G., *Diritto penale delle tecnologie informatiche*, Utet, Torino, 1999
- PICOTTI, L., *Commento all'art. 3 l. 23 dicembre 1993, n. 547*, in *Leg. pen.*, 1996, pp. 62 ss.
- PICOTTI, L, *Reati informatici*, in *Enc. giur. Treccani*, Roma, 1999, pp. 1 ss.
- PIERRO, G., *Introduzione allo studio dei mezzi di ricerca della prova informatica*, in *Dir. pen. proc.*, 2011, pp. 1516 ss.
- PIO, E., *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite*, in *Parola alla difesa*, 2016, pp. 160 ss.
- PISANI, V., *Atti della polizia giudiziaria*, in *Enc. giur. Treccani*, 2007, pp. 1 ss.
- PITTELLI, G., – COSTARELLA, F., *Ancora in tema di* chat "pin to pin" *sul sistema telefonico* BlackBerry, in *Arch. pen. web*, n. 1, pp. 1 ss.
- PITTIRUTTI, M., *Profili processuali della prova informatica*, in *'Incontri ravvicinati' con la prova penale. Un anno di seminari a Roma Tre*, a cura di L. Marafioti – G. Paolozzi, Giappichelli, Torino, 2014, pp. 49 ss.

- PIZZETTI, F., Privacy *e diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016
- PONZANELLI, G., *Scienza, verità e diritto: il caso Bendectin*, in *Foro it.*, 1994, IV, cc. 184 ss.
- PULITANÒ, D., *Due approcci opposti sui rapporti tra Costituzione e Cedu in materia penale. Questioni lasciate aperte da Corte cost. n. 49/2015*, in *Dir. pen. cont.*, 2015, n. 2, pp. 318 ss.
- PULVIRENTI, A., *Sequestro e* internet*: un difficile binomio tra "vecchie" norme e "nuove" esigenze*, in *Proc. pen. giust.*, 2015, n. 1, pp. 111 ss.
- RAFARACI, T., *Ricognizione informale dell'imputato e (pretesa) fungibilità delle forme probatorie*, in *Cass. pen.*, 1998, pp. 1737
- RICCI, G.F., *Le prove atipiche*, Giuffrè, Milano, 1999
- RICCI, G. F., *Nuovi rilievi sul problema della «specificità» della prova giuridica*, in *Riv. trim. dir. proc. civ.*, 2000, pp. 1129
- RIVELLO, P.P., *La prova scientifica*, Giuffrè, Milano, 2014
- ROSSI VANNINI, A., *La criminalità informatica: le tipologie di* computer crimes *di cui alla L. 547/93 dirette alla tutela della riservatezza e del segreto*, in *Riv. trim. dir. pen. ec.*, 1994, pp. 427 ss.
- RUGGERI, F., *Profili processuali nelle investigazioni informatiche*, in *Il diritto penale dell'informatica nell'epoca di internet*, a cura di L. Picotti, Cedam, Padova, 2004, pp. 153
- SALVADORI, I., *Quando un* insider *accede abusivamente ad un sistema informatico o telematico? Le sezioni unite precisano l'ambito di applicazione dell'art. 615* ter *c.p.*, in *Riv. trim. dir. pen. econ.*, 2012, pp. 369 ss.
- SARZANA DI SANT'IPPOLITO, C., *Informatica e diritto penale*, Giuffrè, Milano, 1994
- SARZANA DI SANT'IPPOLITO, C., *La convenzione europea sulla cibercriminalità*, in *Dir. pen. proc.*, 2002, pp. 903 ss.
- SARZANA DI SANT'IPPOLITO, C., *Informatica, internet e diritto penale*, Giuffrè, Milano, 2010
- SBISÀ, F., *Cenni sul* computer *come strumento di prova nel processo penale*, in *Foro ambr.*, 2000, pp. 95 ss.
- SCHENA, G., *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*, in *Cass. pen.*, 2016, pp. 296 ss.

- SCIARABBA, V., *Nuovi punti fermi (e questioni aperte) nei rapporti tra fonti e corti nazionali ed internazionali*, in *Giur. cost.*, 2007, pp. 3579 ss.
- SELVAGGI, E., *Art. 312*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. IV, pp. 360 ss.
- SELVAGGI, E., *Art. 316*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. IV, pp. 332 ss.
- SELVAGGI, E., *Artt. 253-265*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, Torino, 1990, vol. II, pp. 733 ss.
- SIGNORATO, S., *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.*, 2012, pp. 580 ss.
- SIGNORATO, S., *Contrasto al terrorismo e* data retention*: molte ombre e poche luci*, in *Il nuovo 'pacchetto' antiterrorismo*, a cura di R. E. Kostoris – F. Viganò, Giappichelli, Torino, 2015, pp. 75 ss.
- SIGNORATO, S., *Il trattamento dei dati personali per fini di prevenzione e repressione penale*, in *Riv. dir. proc.*, 2015, pp. 1484 ss.
- SIGNORATO, S., *Le misure di contrasto in rete al terrorismo:* Black List*, inibizione dell'accesso ai siti, rimozione del contenuto illecito e interdizione dell'accesso al dominio* internet, in R. E. Kostoris – F. Viganò, *Il nuovo 'pacchetto' antiterrorismo*, Giappichelli, Torino, 2016, pp. 55 ss.
- SINISCALCO, M., *Domicilio (violazione di)*, in *Enc. dir*, Giuffrè, Milano, 1964, pp. 871 ss.
- SIRACUSANO, D., *Studio sulla prova delle esimenti*, Giuffrè, Milano, 1959
- SIRACUSANO, D., *Prova, III) nel nuovo codice di procedura penale*, in *Enc. giur. Treccani*, Roma, 1992, pp. 1 ss.
- SPANGHER, G., *La riforma Orlando della giustizia: prime riflessioni*, in *www.penalecontemporaneo.it*
- STERLOCCHI, C., *Gli* Standards *di ammissibilità della prova penale scientifica nel processo statunitense*, in *Scienza processo penale. Nuove frontiere e vecchi pregiudizi*, a cura di C. Conti, Giuffrè, Milano, 2011, pp. 397 ss.
- STRACUZZI, A., Data retention*: il faticoso percorso dell'art. 132 codice* privacy *nella disciplina della conservazione dei dati di traffico* in *Dir. inf.*, 2008, pp. 585 ss.

- STRAMAGLIA, M., *Il pedinamento satellitare: ricerca ed uso di una prova "atipica"* in *Dir. pen. proc.*, 2011, pp. 213 ss.
- TAGLIAFERRO, M.D., *Il documento informatico nell'ordinamento vigente*, in *Documento informatico e firma digitale. Aspetti penali*, a cura di E. Palmieri, Giappichelli, Torino, 2001, pp. 719 ss.
- TAGLIARO, F. – D'ALOJA, E. – FREDERICK, S.; *L'ammissibilità della «prova scientifica» in giudizio e il superamento del* Frye standard*: note sugli orientamenti negli USA successivi al caso* Daubert v. Merrell Dow Pharmaceuticals, inc., in *Riv. it. med. leg.*, 2000, pp. 719 ss.
- TARUFFO, M., *Studi sulla rilevanza della prova*, Cedam, Padova, 1970
- TARUFFO, M., *La prova dei fatti giuridici. Nozioni generali*, in *Trattato di diritto civile e commerciale*, già diretto da A. Cicu – F. Messineo, continuato da L. Mengoni, Giuffrè, Milano, 1992, vol. III, t. 2, sez. 1
- TARUFFO, M., *Le prove scientifiche nella recente esperienza statunitense*, in *Riv. trim. dir. proc. civ.*, 1996, pp. 219 ss.
- TARUFFO, M., *La prova scientifica nel processo civile*, in *Riv. trim. dir. proc. civ.*, 2005, pp. 1179 ss.
- TARUFFO, M., *Prova scientifica (diritto processuale civile)*, in *Enc. dir.*, Giuffrè, Milano, 2008, ann. II, t. I, pp. 965 ss.
- TESTAGUZZA, A., *I sistemi di controllo remoto: fra normativa e prassi*, in *Dir. pen. proc.*, 2014, pp. 759 ss.
- TESTAGUZZA, A., Chat BlackBerry*: il sistema "pin-to-pin". Nascita di un nuovo paradiso processuale*, in *Arch. Pen. web*, 2016, n. 1, pp. 1 ss.
- TESTAGUZZA, A., Exitus acta probat *"Trojan" di Stato: la composizione di un conflitto*, in *Arch. pen. web*, 2016, n. 2, pp. 1 ss.
- TONINI, P., *Prova scientifica e contraddittorio*, in *Dir. pen. proc.*, 2003, pp. 1459 ss.
- TONINI, P., *La prova scientifica: considerazioni introduttive*, in *La prova scientifica nel processo penale*, a cura di P. Tonini, Ipsoa, Milano, 2008, pp. 1 ss.
- TONINI, P., *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, pp. 401 ss.
- TONINI, P., *La Cassazione accoglie i criteri* Daubert *sulla prova scientifica. Riflessi sulla verifica delle massime d'esperienza*, in *Dir. pen. proc.*, 2011, pp. 1341 ss.

- TONINI, P., *Il diritto alla prova scientifica a dieci anni dalla sentenza Franzese*, in *Proc. pen. giust.*, 2012, n. 4, pp. 1 ss.
- TONINI, P., *Il documento informatico: problematiche civilistiche e penalistiche a confronto*, in *Corr. giur.*, 2012, pp. 432 ss.
- TONINI, P., *La prova documentale*, in P. Tonini – C. Conti, *Il diritto delle prove penali*, Giuffrè, Milano, 2012, pp. 353 ss.
- TORRE, M., *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. proc.*, 2015, pp. 1163 ss.
- TRANCHINA, G., *Sequestro II) sequestro penale*, in *Enc. giur. Treccani*, Roma, 1994, pp. 1 ss.
- TRAVERSO, C. E., *La nozione del concetto di domicilio nell'art. 14 della Costituzione*, in *Studi in onore di Antonio Amorth*, Giuffrè, Milano, 1982, vol. II, pp. 585 ss.
- TRIGGIANI, V. N., *Il «diritto alla prova» nel nuovo codice di procedura penale*, in *Arch. n. proc. pen.*, 1991, pp. 667 ss.
- TROGU, M., *Le indagini svolte con l'uso di programmi spia (*trojan horse), in *La giustizia penale nella rete*, a cura di R. Flor – D. Falcinelli – S. Marcolini, DIPLAP EDITOR, Milano, 2015, pp. 67 ss.
- TROGU, M., *Come si intercettano le* chat pin to pin *tra dispositivi* Blackberry*?*, in *Proc. pen. giust.*, 2016, n. 3, pp. 73 ss.
- TROISI, P., *Sequestro probatorio del* computer *e segreto giornalistico*, in *Dir. pen. proc.*, 2008, pp. 763 ss.
- TROISIO, C., *Corrispondenza (libertà e segretezza della)*, in *Enc. giur. Treccani*, Roma, 1988, pp. 1 ss.
- TRONCONE, P., *La tutela penale del documento dematerializzato tra vicende normative e nuove aspirazioni sistematiche*, in *Riv. pen.*, 2008, pp. 1277 ss.
- UBERTIS, G., *Azione, II) azione penale*, in *Enc. giur. Treccani*, Roma, 1988, pp. 1 ss.
- UBERTIS, G., *Documenti e oralità*, in *Evoluzione e riforma del diritto e della procedura penale, 1945-1990: studi in onore di Giuliano Vassalli*, a cura di M.C. Bassiouni – A.R. Latagliata – A.M. Stile, Giuffrè, Milano, 1991, vol. II, pp. 297 ss.
- UBERTIS, G., *La prova scientifica e la nottola di Minerva*, in *La prova scientifica nel processo penale*, a cura di L. De Cataldo Neuburger, Cedam, Padova, 2007, pp. 83 ss.

- UBERTIS, G., *La prova penale. Profili giuridici ed epistemologici*, Utet, Torino, 1995
- UBERTIS, G., *Il giudice, la scienza e la prova*, in *Cass. pen.*, 2011, pp. 4111 ss.
- UBERTIS, G., *La "rivoluzione d'ottobre" della Corte costituzionale e alcune discutibili reazioni*, in *Cass. pen.*, 2012, pp. 19 ss.
- UGOCCIONI, L., *Commento all'art. 11 l. 23 dicembre 1993, n. 547*, in *Leg. pen.*, 1996, pp. 140 ss.
- VACIAGO, G., Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, Torino, 2012
- VALENTINI, C., *I poteri del giudice dibattimentale nell'ammissione della prova*, Cedam, Padova, 2004
- VASSALLI, G., *Il diritto alla prova nel processo penale*, in *Riv. it. dir. proc. pen.*, 1969, pp. 3 ss.
- VELANI, L. G., *Nuove tecnologie e prova penale: il sistema d'individuazione satellitare g.p.s.*, in *Giur. it.*, 2003, pp. 12 ss.
- VELANI, L. G., *Trojan horse, strumenti investigativi e diritti fondamentali: alla ricerca di un difficile equilibrio*, in *Parola alla difesa*, 2016, pp. 173 ss.
- VELE, A., *Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma*, Cedam, Padova, 2011
- VENTURA, N., *Sequestro preventivo*, in *Dig. pen.*, Utet, Torino, 2004, agg. II, pp. 750 ss.
- VERONESI, P., *Per un'interpretazione costituzionale del concetto di "domicilio"*, in *Ann. univ. Ferrara*, 2003, pp. 105 ss.
- VICOLI, D., *Riflessioni sulla prova scientifica: regole inferenziali, rapporti con il sapere comune, criteri di affidabilità*, in *Riv. it. med. leg.*, 2013, pp. 1239 ss.
- VIGANÒ, F., *Fonti europee e ordinamento italiano*, in *Europa e diritto penale*, a cura di F. Viganò – O. Mazza, Ipsoa, Milano, 2011, pp. 4 ss.
- VIGANÒ, F., *Osservazioni a primissima lettura su Corte cost., sent. 26 marzo 2015, n. 49, Pres. Criuscolo, Red. Lattanzi, in materia di confisca di terreni abusivamente lottizzati e proscioglimento per prescrizione*, in *Dir. pen. cont.*, 2015, n. 2, pp. 333 ss.
- VIOLA BERRUTI, L., Cyber terrorism*: esigenze di tutela preventiva e nuovi strumenti di contrasto* in *www.lalegislazionepenale.eu*
- ZACCHÈ, F., *La prova documentale*, Giuffrè, Milano, 2012

- ZACCHÈ, F., *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.*, 2013, n. 4, pp. 103 ss.
- ZAGREBELSKY, V., *Corte cost. n. 49 del 2015, giurisprudenza della Corte europea dei diritti umani, art. 117 Cost., obblighi derivanti dalla ratifica della Convenzione*, in www.osservatorioaic.it, pp. 1 ss.
- ZAMPERINI, V., *Impugnabilità del sequestro probatorio di dati informatici*, in *Dir. pen. proc.*, 2016, pp. 508 ss.
- ZAPPALÀ, E., *Il principio di tassatività dei mezzi di prova nel processo penale*, Giuffrè, Milano, 1982
- ZIRULIA, S., *Amianto e responsabilità penale: causalità ed evitabilità dell'evento in relazione alle morti derivate da mesotelioma pleurico*, in *www.penalecontemporaneo.it*
- ZONARO, M., *Il Trojan – Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento d'intercettazione*, in *Parola alla difesa*, 2016, pp. 163 ss.