QUESITI

GIANFEDERICO CECANESE

Dinamiche probatorie e moderne tecnologie informatiche. Il virus "spia" nel processo penale tra incertezze dogmatiche, orientamenti giurisprudenziali e nuovi scenari normativi

Le Sezioni unite della Corte di cassazione, di recente, si sono occupate di un tema di viva e palpitante attualità ontologicamente connesso all'enorme capacità invasiva del captatore informatico e al suo ampio impiego nelle indagini preliminari delimitandone lo spazio operativo. Purtuttavia, le peculiarità di questa s*pecie*s di prova scientifica non ci consentono, allo stato, di dare una definizione corretta di questo atipico strumento vista la possibilità di atteggiarsi in differenti modi: intercettazione, ispezione e perquisizione finalizzate a sequestrare i dati rilevati all'insaputa del soggetto interessato: né, tantomeno, la riforma Orlando ha offerto soluzioni definitive alle differenti opzioni interpretative mosse dalla critica.

The United States Sections of the Court of Cassation have recently dealt with a theme of vibrant and timely news ontologically linked to the enormous invasive capacity of the computer capture and its extensive use in preliminary investigations by delimiting its operational space.The peculiarities of this type of scientific evidence, however, do not allow us, in the state, to give a correct definition of this atypical instrument, given the possibility of approaching in different ways: interception, inspection and search to seize the data detected without the knowledge of interested person: nor did Orlando reform offer definitive solutions to the different interpretative options triggered by critics.

1. *Premessa: scenari probatori e nuove tecnologie.* L'osservatore assiste, quasi quotidianamente, a trasmissioni televisive, interviste e articoli di giornali ove, in relazione a gravi delitti, le macchie di sangue, le impronte e le tracce biologiche rinvenute sulla scena del crimine, vengono definite "*prove schiaccianti*", "*inconfutabili*", "*incontrovertibili*", ecc.

Si tratta, in realtà, della falsa sensazione di oggettività che connota la "*cieca*" fiducia nella c.d. "*prova scientifica*" la quale apparendo, *prima facie*, evidente, annichilisce il senso critico.

Da alcuni anni, tale tendenza ha investito progressivamente anche un'altra fonte di informazioni utili allo sviluppo delle indagini: i dati digitali, informatici e telematici.

Per la precisione, ad essere evocati spesso non sono nemmeno i dati, quanto i *computers*, gli *smartphone*, i *tablet*, i sistemi di navigazione *gps* e tutti gli altri dispositivi digitali che ne costituiscono solo l'apparente involucro[1].

L'avvento di *Internet* e delle nuove tecnologie informatiche[2] ha, di fatto, determinato una rivoluzione tecnologica e delle relazioni interpersonali[3] al punto che i dispositivi informatici sono diventati essenziali per le più diverse esigenze dell'utente.

Evidenti sono i riflessi sul piano del diritto ed, in particolare, dell'accertamento penale: da un lato, gli strumenti informatici sono d'ausilio per la commissione di particolari reati e, dall'altro, le memorie dei dispositivi costituiscono altrettanti archivi di informazioni di cui l'organo inquirente non può fare a meno per la ricostruzione della vicenda: le c.d. indagini informatiche hanno, invero, carattere trasversale e non coinvolgono soltanto i reati che abbiano ad oggetto, o la cui commissione avvenga per il tramite di sistemi informatici (c.d. reati informatici)[4], ben potendo rilevare per l'accertamento di illeciti privi di una dimensione tecnologica come, ad esempio, l'omicidio o la violenza sessuale[5].

---

[1] Per un approfondimento della problematica, cfr., A. GAMMAROTA, *Danneggiamento di sistema informatico della P.A. e informatica forense: un caso*, in P. POZZI, R. MASOTTI, M. BOZZETTI, (a cura di), *Crimine virtuale, minaccia reale*, Roma, 2004, 207 ss. Tra gli altri, v. P. GALDIERI, *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997, 34 ss.; G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 211; L. PICOTTI, *Reati informatici*, in *Enc. giur.*, Agg. VIII, Roma, 2000, 1.

[2] L'informatica, unitamente all'elettronica e alle telecomunicazioni, unificate sono denominate *Information and Communication Technology (ICT)* e rappresentano quella disciplina che ha dato vita e sviluppo alla terza rivoluzione industriale attraverso quella che è comunemente nota come rivoluzione informatica. Cfr. M. LUBERTO, G. ZANETTI. *Il diritto penale nell'era digitale. Caratteri, concetti e metafore,* in *Ind. pen.*, 2008, 497.

[3] Secondo J. RUX, *Ausforschungprivater Rechnerdurch die Polizei-und Sicherheitsbehörden-Rechtsfragender "Online-Durchsuchung"*, in *JZ*, 2007, 285 ss., all'invenzione della ferrovia nessun'altra rivoluzione tecnologica ha prodotto un cambiamento così rapido e radicale nei comportamenti umani come *internet* e la tecnologia.

[4] Si vedano L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, 86 ss.; C. SARZANA, DI S. IPPOLITO, *Informatica, Internet e diritto penale*, 3ªed., Milano, 2010, 61 ss.

[5] Si pensi a titolo esemplificativo al caso di Garlasco, dove la prova d'alibi si basava essenzialmente sull'utilizzo del *computer* in una fascia oraria, oppure al c.d. stupro della Caffarella, in cui i due rumeni inizialmente arrestati sono stati liberati perché scagionati dal test del *dna* e dalla mappatura del traffico telefonico.

Al tempo stesso, però, occorre sottolineare che la "*realtà digitale*", quale oggetto di indagine, si connota per la sua natura volatile ed alterabile dei dati digitali e fa sorgere rilevanti questioni sulla loro corretta acquisizione, conservazione ed utilizzazione all'interno del contesto processuale.
Essendo connotati dall'immaterialità i dati informatici si sostanziano in informazioni espresse in codice binario (*bit* con sequenze di 0 e 1) e, per essere fruibili, devono essere incorporati su un supporto fisico[6].
Per "*sfuggire*" all'occhio dell'inquirente, in molti casi, essi sono salvati su *server* dislocati in Paesi diversi rispetto a quello dove si svolgono le indagini ponendo, quindi, ulteriori e seri problemi di cooperazione giudiziaria che richiedono un continuo aggiornamento degli strumenti di cooperazione ma, anche, uno sforzo di armonizzazione delle varie normative investigative, in modo da evitare una sorta di "*far west tecnologico*" in cui ogni Stato conduce indagini oltre la propria sovranità.
Dunque, affinché l'accertamento possa assumere le caratteristiche dell'affidabilità è necessario garantire la genuinità del dato adottando determinate cautele nella ricerca, nella raccolta e nell'analisi: ciò richiede l'adozione di particolari strumenti che, inevitabilmente, minano l'orbita di tutela di taluni diritti protetti e considerati inviolabili in ambito nazionale e sovranazionale.

---

[6] Molto opportunamente, la legge di ratifica della Convenzione di Budapest ha abrogato l'art. 491 *bis* c.p. che considerava documento informatico qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli. Accoglie positivamente tale scelta del legislatore L. PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. proc. pen.*, 2008, 333 ss., il quale ritiene la definizione dell'art. 491 *bis* c.p. inadeguata all'evoluzione tecnologica e in particolare alla c.d. "immaterialità" dei dati digitali, in quanto incentrata sul supporto contenente i dati. Attualmente, l'unica definizione legislativa di documento informatico è contenuta nell'art. 1 del Codice dell'amministrazione digitale (d. lgs. 82/2005), dove esso è descritto come la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (lett. p). Tuttavia, c'è chi dubita che la definizione contenuta nel Codice dell'amministrazione digitale e gli altri requisiti strutturali richiesti per garantire stabilità e identificabilità del documento informatico siano vincolanti nell'ordinamento processuale penale, dove è lo stesso art. 324 c.p.p. a fissare la nozione di documento processualmente rilevante e le relative condizioni di utilizzo. Cfr. P. TONINI, *Documento informatico e giusto processo*, in *Dir. proc. pen.*, 2009, 401; F. ZACCHÈ, *La prova documentale, Milano*, 2012, 86. Questa impostazione può essere fuorviante; infatti, se è vero che l'art. 324 c.p.p., per il richiamo in esso contenuto a qualsiasi altro mezzo, è una norma a struttura aperta, idonea a ricomprendere anche i documenti informatici (ciò è sostenuto, tra gli altri, anche da F. CORDERO, sub *art. 234*, in *Codice di procedura penale commentato*, 2ªed., Torino, 1992, 432), bisogna fare attenzione a nonconfondere il contenuto con il contenitore: i dati digitali non sono prove documentali e non seguono le regole di ammissione per questi dettate dagli artt. 495 c. 3 e 515 c.p.p.: valgono per essi, in considerazione della loro natura volatile e modificabile, regole di raccolta e utilizzo dibattimentale diverse. Sulla necessità di ripensare tutte le comuni regole probatorie, originariamente concepite per le prove tradizionali, si veda O. S. KERR, *Digital Evidence and the New Criminal Procedure*, in *105 Colum. L. Rev.*, 2005, 290 ss. Cfr. anche U. SIEBER, *Straftaten und Strafverfolgungim Internet. Gutachten C zum 69. Deutschen Juristentag*, München, 2012.

Si pensi, ad esempio, allo "*scontro*" tra le varie forme di criminalità e le nuove metodologie investigative di contrasto (pedinamenti satellitari, perquisizioni *on line*, *virus spie*, ecc.) che evoca la necessità di conciliare due fondamentali, ma opposte, esigenze: all'accertamento del fatto fa da contraltare la necessità di tutelare i diritti coinvolti in questa operazione ricostruttiva.
Insomma, il *punctum dolens* è sempre lo stesso e si polarizza nella necessità di trovare un giusto equilibrio tra la tutela della collettività e il rispetto dei diritti della persona[7].
Addirittura, nell'ordinamento tedesco la Corte costituzionale ha "*creato*" una nuova categoria di diritti della personalità in grado di proteggere (ed arginare) l'invasività di strumenti investigativi che si avvalgono delle nuove tecnologie: il riferimento è all'*informationelle Selbstbestimmungsrecht* – il diritto all'autodeterminazione informativa[8] - e al *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrit ätinformationstechnischer Systeme*, ossia il diritto alla "garanzia della segretezza e integrità dei sistemi informatici"[9].
Anche nel nostro Paese, si sente l'esigenza di ampliare la nozione di riservatezza e i profili di garanzia ad essa correlati vista la sua connessione dinamica con l'unico oggetto di tutela: "*la persona nelle sue diverse considerazioni, via via determinate dal suo rapporto con le tecnologie, che non sono solo quelle elettroniche*"[10].
Caratteristica tipica della prova digitale è la sua promiscuità: dati rilevanti per le indagini sono spesso mescolati a dati di carattere personale che, in quanto tali, sono irrilevanti per le esigenze investigative ma possono, se disvelati, essere dirompenti sul piano personale: le indagini informatiche sono, quindi, sempre potenzialmente in grado di pregiudicare la riservatezza degli individui[11].
Di conseguenza, poiché in ambito probatorio, il metodo vale più del risultato e la necessità è quella di conciliare l'esigenza di acquisizione del dato tecnologico con la tutela dell'individuo, il fronte della riflessione non può che proiettarsi sul versante del contraddittorio[12] vero, e proprio, antitodo rispetto all'incertezza connaturata ad una scienza o ad una tecnologia che pretende

---

[7] Cfr., S. LORUSSO, *L'arte di ascoltare e l'investigazione penale tra esigenze di giustizia e tutela della privatezza*, in *Dir. proc. pen.*, 2011, 1397.
[8] *BVerfG*, 15 dicembre 1983, in *BverfGE* 65, 1 ss.
[9] *BVerfG*, 27 febbraio 2008, in *BverfGE* 120, 274.
[10] In questi termini si è espresso S. RODOTÀ, *Il diritto di avere diritti*, Roma, 2012, 317.
[11] F. RUGGIERI, *Profili processuali nelle investigazioni informatiche*, in L. PICOTTI (a cura di),), *Il diritto penale dell'informatica*, Padova, 2004, 158.
[12] Secondo C. CONTI, P. TONINI, *Il diritto delle prove penali*, Milano, 2012, 1, la giustizia s'incontra nel percorso, prima ancora che alla meta.

erroneamente di proporsi come capace di dimostrare i dati in modo assoluto[13].

2. Una seconda riflessione preliminare: le peculiari connotazioni delle indagini e dell'acquisizione dei dati informatici

L'informatica, peraltro, non sfugge alla fallibilità che caratterizza tutte le branche del sapere e l'evidenza elettronica, lungi dall'essere *prova perfetta*, racchiude e riacutizza le criticità già insite nella prova scientifica[14].

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

In tema di *digital evidence,* l'elevata connotazione specialistica della materia, il concreto pericolo di manipolazione o alterazione del materiale probatorio e il rischio di una incontrollata introduzione di una *junk science*, richiedono estrema cautela[16].

L'interprete è chiamato a verificare, con rigore, la compatibilità degli strumenti offerti dal progresso scientifico rispetto ai principi cardine del processo penale, primo fra tutti il diritto di difesa, inviolabile in ogni stato e grado del procedimento[17].

A livello epistemologico, infatti, è necessario, ancora una volta, sfatare il mito della prova scientifica come "*prova perfetta*"[18]: nel processo penale, il sapere

---

[13] Come noto, la crisi dell'equazione tra scienza e episteme si deve al pensiero di K. R. Popper, che segna definitivamente il declino del verificazionismo come metodo gnoseologico. Alla filosofia popperiana si deve la ormai acquisita consapevolezza di una scienza come sapere non più indebitamente certo, ma limitato, incompleto e fallibile. Cfr. K.R. POPPER, *Logica della scoperta scientifica*, Roeino, 1970, 31 ss.

[14] Sullo specifico profilo, diffusamente, S. LORUSSO, *La prova scientifica*, in *La prova penale*, diretta da A. GAITO, Torino, 2008, 295 ss.

[15] Così, F. M. MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2012, 698.

[16] In argomento di recente, v. P. RIVIELLO, *La necessità di evitare l'ingresso della junk scienze nelle aule giudiziarie: un ripensamento circa alcune ricorrenti affermazioni*, in *www.dirittopenalecontemporaneo.it.*

[17] Al riguardo, v., E. LORENZETTO, *Le attività urgenti di investigazione informatica,* in L. LUPARIA (a cura di), *Sistema penale ecriminalità informatica*, Milano, 2012, 137.

[18] In tema ampiamente, cfr. O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi edi elevata specializzazione*, Milano, 2005, 35 ss.

specialistico non deve ergersi a roccia contro la quale sono destinate ad infrangersi le più elementari garanzie partecipative dei soggetti coinvolti nell'accertamento penale, ma deve essere come acqua capace di modellarsi e adeguarsi al contenitore in cui viene versata, un contenitore la cui natura giuridica (e processuale) richiede il rispetto di regole a tutela dei diritti involabili della persona[19]. D'altronde, è la stessa locuzione "prova scientifica" a suggerire una progressione che tenga conto della parola "*scientifica*" – con la quale si rinvia al concetto di scienza – e del termine che la precede, "*prova*", il quale rimanda a norme e principi contenuti nel codice di rito e nella Costituzione.
Ciò nonostante, la scientificità del metodo assume aspetti preminenti rispetto alle necessità ontologicamente connesse all'indagine: ad esempio, diventa difficile immaginare un rilievo scevro da valutazioni di tipo tecnico, ovvero un accertamento tecnico che non sia preceduto da un rilievo dotato di altrettanto tecnicismo.
In ambito digitale, anche la semplice raccolta del dato presuppone una elevata competenza ed una precisa specializzazione, perché richiede delle valutazioni di tipo tecnico in merito alle metodologie da utilizzare, al *software* da applicare, all'*hardware* da impiegare per perseguire lo scopo imposto dalla legge, ossia la tutela dei dati originali[20].
In questo senso si può, allora, sostenere che in ambito digitale il rilievo nasconde, in realtà, un accertamento tecnico o, se si preferisce (ma è lo stesso), che la distinzione tra rilievo e accertamento tecnico, quantomeno in ambito informatico, non ha alcun senso[21].
D'altronde, etimologicamente la parola rilievo deriva dal latino *relevare*, ossia sollevare, ed è composta dal termine *levare*, cioè alzare, preceduto dal prefisso *re*, che sta ad indicare un movimento verso l'alto.

---

[19] Sullo specifico profilo, diffusamente, M. TORRE, *Il captatore informatico*, Milano, 2017, 5.

[20] Cfr., Cass. Sez. I, 26 febbraio 2009, n. 11863, in *Mass. Uff.* n. 243922, secondo cui l'estrazione dei dati contenuti in un supporto informatico, se eseguita da personale esperto in grado di evitare la perdita dei medesimi dati, costituisce un accertamento tecnico ripetibile. *Contra*, Cass., Sez. II, 19 febbraio 2015, n. 8607, in *Mass. Uff.,* n. 263797, secondo cui non dà luogo ad accertamento tecnico irripetibile l'estrazione dei dati archiviati in un computer, trattandosi di operazione meramente meccanica, riproducibile per un numero indefinito di volte.

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

Quindi, il suo esatto significato dovrebbe essere "*togliere da terra*" qualcosa che già di per sé si distingue dal resto delle cose per caratteristiche sue proprie: accertare, invece, viene da "*certo*", che a sua volta deriva dal latino *cernere*, che significa separare, distinguere, qualcosa che in assenza di accertamento rimarrebbe indistinto[22].
Ebbene, anche da questo punto di vista l'attività di estrazione di dati sembrerebbe senz'altro più simile ad un accertamento piuttosto che ad un rilievo.
Per dare una soluzione alla *questio* l'interprete parla più correttamente di rilievi con riferimento a quelle attività nelle quali la componente valutativa, pur esistente, caratterizza il metodo operativo di raccolta dei dati, mentre riserva la qualifica di accertamenti tecnici a quegli atti nei quali la valutazione si traduce in una rielaborazione critica dei dati acquisiti[23].
La vera differenza tra rilevare ed accertare non si colloca nella presenza o nell'assenza dell'aspetto tecnico-valutativo, quanto piuttosto nella diversa fase in cui esso rileva: nei rilievi, la valutazione tecnica attiene alle modalità con le quali, prudentemente, deve essere effettuato l'accertamento; negli accertamenti tecnici, il tecnicismo insiste sul risultato, che rappresenta il frutto di una valutazione.
L'estrazione del dato informatico, rappresenta un tipico esempio di attività caratterizzata da aspetti tecnico-valutativi che, tuttavia, non riguardano il risultato, ma il metodo prescelto al fine di salvaguardare l'integrità dei dati digitali.
Ma, una simile argomentazione, seppur condivisibile in linea teorica, non risolve il problema di fondo: infatti, in ambito digitale la fase di raccolta degli elementi da valutare è rilevante quanto l'analisi, al punto che un errore commesso in fase di estrazione può minare l'attendibilità o, addirittura, l'utilizzabilità dell'evidenza digitale ottenuta.
L'approccio investigativo ad una *scena criminis* informatica non è fatto di improvvisazione ed intuito ma, sempre più spesso, di scienza e tecnica, le quali impongono un protocollo indefettibile.
Ciò ci induce a ritenere che il difficile rapporto tra scienza e diritto processuale penale non coinvolge solo la fase di valutazione e/o validazione della legge scientifica in giudizio, ma, più in generale, il rapporto tra scienza e procedimento penale in tutte le fasi in cui la prima entra in contatto con il secondo.
Il corretto trattamento dell'evidenza digitale, dunque, costituisce un valore assoluto e non è declinabile da parte dell'inquirente, qualunque sia l'attività

[22] Così, A. CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, Torino, 2014, 78.
[23] A. CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, cit., 55.

tecnica posta in essere e chiunque sia il soggetto operante: non esistendo, ad oggi, uno *standard* prestabilito per la metodologia di trattamento ed analisi delle prove informatiche, l'unico principio di riferimento è quello relativo al mantenimento della integrità e non alterazione delle tracce fisiche dei dati informatici: questi devono essere acquisiti al processo ed analizzati attraverso la copia degli stessi ottenuta tramite una procedura che ne assicuri la conformità[24].

La vaghezza del riferimento in cui il legislatore sembra essersi "*trincerato*", senza la previsione di una specifica disciplina di riferimento, ha legittimato la cittadinanza, nel sistema di acquisizione della prova digitale, delle migliori pratiche delineate dalla prassi investigativa: la prova digitale, si accosta in tal modo, alla prova scientifica[25].

3. ***I profili di legittimità dell'acquisizione dei dati digitali.*** Ma quali sono, allora, le conseguenze processuali connesse alla violazione delle *leges artis* ovvero delle *best practices*?

Il quesito è legittimo poiché, nonostante il silenzio serbato dal legislatore sullo specifico versante, è chiaro a tutti che, ove tali prescrizioni non fossero presidiate da conseguenze processuali pregnanti, disquisire in ordine alla loro rilevanza sarebbe del tutto superfluo o inutile.

La risposta a tale interrogativo è tutt'altro che semplice, perché si tratta di valutare le conseguenze, sul piano processuale, della violazione di regole tecniche non inserite nel codice di rito e non standardizzate in ambito scientifico nazionale e internazionale[26].

Nella versione originaria del codice di rito, mancava un esplicito richiamo alle acquisizioni informatiche raccolte in violazione dei requisiti essenziali della genuinità e non alterazione del dato informatico previsti, introdotto solo successivamente dalla legge n. 48/2008[27].

---

[24] Secondo G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici,* in *Sistema penale e criminalità informatica,* 2009, 189, siamo in presenza di norme processuali in bianco. In giurisprudenza, cfr. Cass. Sez. VI, 24 febbraio 2015, n. 65359, in *Mass. Uff.*, n. 264094.

[25] Cfr., G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici,* cit., 190.

[26] Numerose sono le raccolte di linee guida per l'approccio con la c.d. *scena criminis digitale*. Cfr., per un elenco delle migliori pratiche, L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamentodel reato tra progresso scientifico e garanzie fondamentali,* Milano, 2007, 89.

[27] Sulle novità legislativa ed in particolare per un primo commento organico delle stesse, cfr., M.L. DI BITONTO, *La ratifica della Convenzione del Consiglio d'Europa sulcybercrime: profili processuali*, in *Dir. int.*, 2008, 505; L. LUPARIA, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa (L. 18 Marzo 2008 n.48). I profili processuali*, in *Dir. pen. proc.*, 2008, 723.

In verità, il dibattito sulle patologie della prova conseguenti alla raccolta della *digital evidence* in violazione delle *best practices* acquisitive aveva appassionato l'interprete già anteriormente alle modifiche normative del 2008 allorquando si era sostenuto che, pur in assenza di regole *ad hoc* dettate per le indagini informatiche, l'acquisizione contraria ai criteri scientifici comportava, comunque, la nullità dell'atto: infatti, il modo con il quale si raccoglie una certa informazione influisce direttamente sulla capacità dimostrativa della stessa[28].
Pertanto, laddove si agisca in violazione delle misure previste a tutela della conservazione e salvaguardia dei dati originali, l'atto sarebbe da considerarsi nullo riverberando tale effetto sulle prove raccolte[29].
In altre parole, le misure di salvaguardia del dato rappresenterebbero uno speciale requisito che si configura come un elemento costitutivo, sicché la sua imperfezione o la sua assenza impedisce l'integrazione delle medesime e comporta l'invalidità dell'atto, determinandone la nullità (artt. 178 lett. *c*) e 180 c.p.p.)[30]
Pur tuttavia, la soluzione prospettata non si è cristallizzata ma ha, invece, coinvolto altre (e differenti) patologie, toccando, di riflesso, la mera irregolarità e, con migliore calibratura, l'inutilizzabilità delle risultanze, giacché queste ultime sarebbero state inidonee ad assicurare un accertamento attendibile dei fatti di reato[31].
Le prove informatiche acquisite in violazione dei canoni codicistici, devono essere considerate inutilizzabili, per diverse ragioni.
In primo luogo, perchè la legge n. 48/2008 pone un divieto probatorio implicito all'uso di risultanze probatorie informatiche inquinate, cui dovrebbe conseguire l'operatività dell'art. 191 c.p.p[32].

---

[28] L'ardente dibattito dottrinale è ripercorso da F. CAJANI, *Il vaglio dibattimentale della*digitalevidence, in *Arch. pen*, 2013, 837; cfr. anche F. GIUNCHEDI, *Le malpractices nella digital forensics. Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *questa rivista*, 2013, 821, nonché D. LA MUSCATELLA, *La ricerca della prova digitale e la violazione delle best practices: un'attività investigativa complessa tra recenti riforme e principi consolidati*, in *Cib. dir.*, 2011, 221.

[29] Così A. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico otelematico*, in *Dir int*, 2008, 509.

[30] A. VITALE, *op. loc. ult.* cit.

[31] Teorizza tale inutilizzabilità per *unreliability* della prova L. LUPARIA, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale*, in *Dir. int*, 2006, 157; ID., *La disciplina processuale e le garanzie difensive*, cit., 198.

[32] In questo senso L. MARAFIOTI, *Digital evidence e processo penale*, in *Cass. pen.*, 2011, 4522, nonché L. LUPARIA, *Computer crimes e procedimento penale*, cit., 389, secondo cui tale soluzione sarebbe imposta dalla ricorsività di incisi codicistici [...] facenti esplicito e continuo riferimento alla doverosità dell'utilizzo di metodiche che assicurino la genuinità della prova elettronica; d'altra parte, secondo l'Autore, pensare a questa normativa nei termini di una *lex imperfecta*, priva di penalità processuali per la sua violazione, sembra riecheggiare situazioni del passato, superate dalla riforma del 1988, e rischia di ingenerare prassi devianti e perniciose scorciatoie nell'operato dei protagonisti dell'inchiesta penale. Cfr. anche A. MONTI, *La nuova disciplina del sequestro informatico*, cit., 208, nonché S. VENTURINI, *Sequestro probatorio e*

Inoltre, giacché la tutela della genuinità della prova rappresenta l'estrinsecazione del più generale diritto di difesa, costituzionalmente tutelato, la violazione delle regole poste a tutela della sua integrità, dovrebbe condurre ad un'ipotesi di inutilizzabilità delle risultanze per violazione della legge fondamentale[33].

Infine, perchè la sanzione dell'inutilizzabilità segue la inidoneità dimostrativa della fonte di prova acquisita in violazione delle regole, la cui attendibilità è irrimediabilmente compromessa[34].

La *digital evidence* ottenuta o duplicata con metodi impropri o comunque non verificabili equivale, cioè, a un *quid* diverso da quello originariamente rinvenuto e mette a disposizione del giudice un dato adulterato.

Sotto un profilo generale, dunque, quel *deficit* tecnico nell'acquisizione del dato informatico andrebbe ricondotto a una situazione di inidoneità probatoria del risultato in sé e di qualsiasi ulteriore mezzo finalizzato ad analizzarlo. Ne deriverebbe, quindi, il dovere del giudice di escludere già in fase di ammissione della prova (art. 190 c.p.p.) l'evidenza digitale rilevata, con conseguente inutilizzabilità della stessa ovvero della sua successiva analisi tecnica in quanto acquisite, entrambe, in violazione di un divieto stabilito dalla legge (art. 191, co. 1, c.p.p.)[35].

Vi sono, naturalmente, esegesi antitetiche rispetto a quella appena richiamata.

In particolare, l'assenza di una espressa sanzione conseguente alla mancata osservanza dei canoni dettati dalla legge n. 48/2008 ha portato la dottrina a ritenere che l'inosservanza delle misure tecniche idonee ad assicurare la salvaguardia della genuinità dei dati e delle informazioni raccolte incida sulla valutazione della prova ed in particolare solo sulla fondatezza dei risultati acquisiti senza generare alcuna invalidità[36].

---

fornitori di servizi telematici, in L. LUPARIA (a cura di), *Internet Provider e giustizia penale*, cit., 124.

[33] In quest'ottica, circa l'esistenza, accanto all'inutilizzabilità "patologica", di una inutilizzabilità "costituzionale", v. M. BERGONZI PERRONE, *Il mancato rispetto delle disposizioni della Legge n. 48 del 2008 in tema di acquisizione probatoria informatica: per una ipotesi sanzionatoria non prevista esplicitamente dal dato normativo*, in *Cib. dir.*, 2013, 128.

[34] Sullo specifico profilo, cfr., E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit. 135.

[35] E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit., 135. Viceversa, secondo D. LA MUSCATELLA, *La genesi della prova digitale: analisi prospettica dell'ingresso dell'informatica forense nel processo penale*, in *Cib. dir.*, 2012, 390, l'attendibilità della prova quale criterio per la sua ammissibilità (ed in seguito per la sua valutazione) troverebbe un referente codicistico nell'art. 189 c.p.p. Tale disposizione non riguarderebbe soltanto la prova atipica, ma costituirebbe norma generale connaturata al processo accusatorio e, dunque, relativa a tutti i mezzi di ricerca della prova. Si tratta, com'è agevole intuire, di una ricostruzione debitrice, per un verso, di quella inutilizzabilità per *unreliability* già teorizzata antecedentemente alla legge n. 48/2008 e, per altro verso, della teoria anglosassone della *unfairevidence*.

[36] Così G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, cit., 190.

Di qui, la necessità che il giudice, al più, debba cercare elementi esterni di riscontro al materiale probatorio informatico "*debole*" in quanto non genuino ovvero alterato.
Trattasi di opzione interpretativa condivisa anche da qualche giudice di merito.
Infatti, già nel *leading case* "*Vierika*"[37] il giudice enunciò una *regula iuris* destinata a consolidarsi in giurisprudenza: vale a dire che il giudice non ha il potere di escludere *a priori* i risultati di una tecnica informatica utilizzata ai fini forensi solo perché alcune fonti ritengono che ne esistano di più corrette, in assenza della allegazione di fatti che suggeriscano che si possa essere astrattamente verificata nel caso concreto una qualsiasi forma di alterazione dei dati e senza che venga indicata la fase delle procedure durante la quale si ritiene essere avvenuta la possibile alterazione[38].
Tesi, questa, decisamente suggestiva che non può essere condivisa giacché, si tratta di un *onus probandi* del tutto anomalo che si risolve in una vera e propria *probatio diabolica*, posto che il dato originario, dopo la modifica, risulta per lo più irrecuperabile[39].
Tra l'altro, anche se il metodo utilizzato non dovesse ritenersi conforme alla miglior pratica scientifica, si perverrebbe, comunque, a risultati che rientrano nell'orbita della libera valutazione del giudice.
Tuttavia, di recente, si sono registrate timide aperture da parte dell'organo di legittimità il quale ha ritenuto legittima la possibilità di trovarsi di fronte ad un dato inutilizzabile allorchè la raccolta sia avvenuta in modo non del tutto genuino[40].
Anche se in giurisprudenza prevale la tesi della sostanziale irrilevanza del vizio.

---

[37] Questa, in breve, la vicenda: un consulente informatico era imputato dei reati previsti dagli artt. 615-*ter* e 615-*quinquies* c.p. per aver messo in circolazione un *virus* informatico denominato "Vierika". Il *worm* si diffondeva attraverso l'invio inconsapevole di *e-mail* da parte di quanti avessero incautamente aperto l'allegato "infetto" a loro pervenuto. Ben lungi dall'essere una semplice immagine digitale, l'accesso al *file* provocava una serie di modificazioni del sistema operativo fra cui la modifica della pagina iniziale del *browser* di navigazione. All'identificazione dell'imputato si era pervenuti a seguito dell'acquisizione ditracce informatiche registrate nel *server* dell'*Internet Service Provider*, mediante le quali era stato identificato l'amministratore del sito in questione. Un' approfondita disamina del *dictum* si rinviene in L. LUPARIA, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale*, in *Dir. int.*, 2006, 156.
[38] Così Trib. Bologna, 22 dicembre 2005, n. 1823, in *Dir. int.*, 2005, 153.
[39] Cfr, L. MARAFIOTI, *Digital evidence e processo penale*, cit., 4521; in questo senso anche L. LUPARIA, *op. loc. ult. cit.*, 158, il quale ritiene che simile onere della prova si collochi al di fuori dell'architettura sistematica del nostro ordinamento processuale.
[40] Ad esempio Cass. Sez. III, 16 ottobre 2014, n. 43304, *inedita*.

In questa prospettiva, allora, in ambito di *digital evidence*, il libero convincimento diventa viatico per legittimare un approccio antiformalistico in tema di prova[41].

Va, dunque, ribadito che la soluzione della questione deve essere ancorata alla natura fragile e volatile del materiale informatico da cui scaturisce un inevitabile corollario: l'impiego di metodi di acquisizione scorretti muta la natura stessa della prova la quale perde la sua intrinseca idoneità dimostrativa, in quanto irrimediabilmente contaminata.

Il discorso non muta con riferimento alla *digital evidence*: eventuali violazioni nelle modalità di apprensione del dato incidono, inevitabilmente, sull'essenza del medesimo, poiché il contenuto viene modificato[42].

I canoni che connotano il dato informatico - genuinità e non alterazione – assumono, quindi, diversa valenza e vanno considerati non già mere disposizioni d'auspicio, ma veri e propri divieti impliciti presidiati dalla sanzione dell'inutilizzabilità.

In questo modo si risolve anche un'ulteriore aspetto ontologicamente connesso alla *questio* in oggetto, ossia la ricerca del parametro cui ancorare la declaratoria di invalidità: questo va, necessariamente, individuato sia nel dovere di "*adottare misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*" (artt. 244, comma 2, 247, comma 1 *bis*, 352, comma 1 *bis*, e 354, comma 2, c.p.p.), sia nell'obbligo di acquisire i dati informatici mediante "*procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità*" (artt. 254 *bis* e 260, comma 2, c.p.p.).

Ciò precisato, l'attenzione si sposta sulla possibilità, assai dibattuta in dottrina, di configurare divieti probatori impliciti.

Ebbene, sul punto, appare opportuno recuperare quell'insegnamento giurisprudenziale secondo cui l'inutilizzabilità, (art. 191, comma 1, c.p.p) può derivare soltanto dalla violazione di un divieto di acquisizione che, quando non sia esplicito, può riconoscersi come implicito in relazione alla natura o all'oggetto della prova[43].

---

[41] Così L. MARAFIOTI, *Digital evidence e processo penale*, cit., 4521.

[42] In quest'ottica, sia pure con riferimento, più in generale, al tema della *scientificevidence*, C. CONTI, *Il volto attuale dell'inutilizzabilità: derive sostanzialistiche e bussola della legalità*, in *Dir. pen. proc.*, 2010, 790.

[43] Cass., Sez. I, 27 maggio 1994, n. 7491, in *Arch. n. proc.*, 1994, 504, secondo cui atteso il testuale tenore dell'art. 191, comma primo, c.p.p., il quale sancisce la inutilizzabilità delle prove "acquisite in violazione dei divieti stabiliti dalla legge", deve ritenersi che detta inutilizzabilità possa derivare, in difetto di espressa, specifica previsione, soltanto dalla illegittimità in sè della prova stessa, desumibile dalla norma o dal complesso di norme che la disciplinano, e non invece soltanto dal fatto che la prova, in sè e per sè legittima,

Ed appunto, come si è avuto modo di illustrare, le interpolazioni della legge n. 48/2008 tutelano proprio la natura volatile della prova informatica da possibili involontarie contraffazioni.

L'assunto che precede è avvalorato dall'analisi delle conseguenze cui approda quella critica che assegna al giudice il compito di valutare l'idoneità probatoria delle risultanze digitali apprese mediante procedure scientificamente scorrette. Per tale via, invero, si assegna al magistrato un compito estremamente arduo di verifica, caso per caso, in relazione alla sussistenza o meno di condotte scorrette da parte dell'organo inquirente che abbiano o meno compromesso l'attendibilità del materiale probatorio[44].

Dunque, una ricostruzione di tal guisa che, ben lungi dal restituire al giudice la doverosa funzione di *gate-keeper* rispetto all'ingresso della *junk science* nel processo, delega sempre più al sapere esterno dell'esperto la decisione[45].

Certo, *de jure condendo*, una riforma che chiarisca l'effettiva portata precettiva delle *regula agendi* dettate nei confronti di coloro che operano sul dato informatico sarebbe auspicabile.

Ma, allo stato, la categoria dei divieti impliciti evocati dalla l. n. 48/2008 sembra perseguire al meglio la *ratio legis* ad essa sottesa, nonché l'unica in grado di rispettare il principio garantistico secondo il quale le regole di esclusione devono garantire l'attendibilità dell'accertamento e tutelare il metodo di formazione delle prove da eventuali abusi[46].

---

sia stata acquisita irritualmente. Nè in contrario potrebbe farsi richiamo all'art. 526 c.p.p., secondo il quale il giudice non può utilizzare, ai fini della deliberazione, prove diverse da quelle legittimamente acquisite nel dibattimento. Non potendosi, infatti, prescindere, nella interpretazione di detta ultima norma, dall'esigenza del suo inserimento in un sistema coerente e armonico che vede nettamente distinte le categorie della nullità e della inutilizzabilità (distinzione che verrebbe di fatto meno qualora ogni inosservanza formale, anche se non sanzionata da nullità ovvero sanzionata da nullità non più deducibile o comunque sanata venisse poi a rilevare come causa di inutilizzabilità), deve necessariamente ritenersi che per "prove diverse da quelle legittimamente acquisite" debbono intendersi non tutte le prove le cui formalità di acquisizione non siano state osservate, ma solo quelle che non si sarebbero potute acquisire proprio a cagione dell'esistenza di un espresso o implicito divieto.

[44] Si ricordino, a tal proposito, le icastiche osservazioni di M.R. DAMASKA, *Il diritto delle prove alla deriva*, trad. it., Bologna, 2003, 52, secondo cui non è forse il giudice medio [...] perplesso riguardo ad arcane intuizioni scientifiche? La scienza moderna pone sempre più di fronte a tutti i giudici "generalisti", abbiano essi o no una preparazione giuridica, informazioni che solo degli esperti possono capire senza difficoltà. Per quanto attiene alle informazioni scientifiche, quindi, sia i giudici professionali sia i laici sono dei profani, ugualmente in difficoltà alla ricerca di spiegazioni.

[45] A tal proposito, v., ancora, le premonitrici considerazioni di M.R. DAMASKA, *op. cit.*, p. 215, rileva che dover fare affidamento su informazioni scientifiche impenetrabili aumenta le contraddizioni rispetto alla possibilità che l'organo giudicante analizzi la prova sulla base dei processi cognitivi ordinari. Una delle pietre angolari del diritto delle prove europeo moderno, e cioè il principio della libera valutazione delle prove, dovrà essere ripensato e riconcettualizzato nel prossimo futuro.

[46] Così F.M. GRIFANTINI, *Inutilizzabilità* (voce), in *Dig. disc. pen.*, VII, 1993, 2471. In quest'ottica, v. anche le annotazioni di L. LUPARIA, *Le scienze penalistiche nella "tempesta" digitale. Quali approdi?*, in

4. *Alla ricerca di un delicato equilibrio: l'assetto minimo delle garanzie fondamentali.* L'invasività delle metodologie di acquisizione dei dati digitali e informatici pone diversi interrogativi sulla correlazione con i diritti e le garanzie del giusto processo. L'ambito operativo della tutela della libertà dell'individuo è stato circoscritto da una nota sentenza della Corte costituzionale con la quale è stato precisato che "a*ttività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito*[47].

Il *dictum* è chiaro: da un lato, si è voluto sottolineare che il diritto alla libertà personale (art. 13 Cost.) assume una posizione prioritaria tra i diritti inviolabili dell'uomo, riconosciuti e garantiti dall'art. 2 Cost. a salvaguardia del pieno svolgimento della personalità di ciascuno, fungendo da presupposto di tutti gli altri diritti di libertà, in quanto capace di condizionarli a livello operativo, rendendone possibile la piena esplicazione[48]; dall'altro, (e il versante coinvolge anche il dato informatico) evidenti sono le interconnessioni con altre garanzie come la libertà del domicilio (art. 14 Cost.), la libertà e la segretezza delle comunicazioni (art. 15 Cost.) e la libertà di circolazione (art. 16 Cost.) anch'esse inviolabili e complementari alla piena tutela della libertà personale[49].

Si tratta di diritti che garantiscono all'individuo indipendenza e capacità di autodeterminarsi nella vita di relazione, sottraendo al controllo e all'interferenza da parte di terzi, determinati aspetti della vita privata: tuttavia,

---

questa rivista, 2013, 880: Id., *Computer crimes e procedimento penale*, cit., 390.

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

[48] Al riguardo, V. GREVI, *Libertà personale dell'imputato e costituzione*, Milano, 1976, 1. Si veda anche il fondamentale studio di G. VASSALLI, *La libertà personale nel sistema delle libertà costituzionali*, in *Scritti giuridici in memoria di P. Calamandrei*, V, Padova, 1958, 355.

[49] P. BARILE, E. CHELI, voce *Corrispondenza (libertà di),* in *Enc. dir.*, vol. X, Milano, 1962, 744, secondo cui tutte le libertà costituzionali si manifestano come conseguenza della tutela della libertà personale, ma la libertà di domicilio e quella di corrispondenza più di ogni altra integrano e specificano la sfera normativa dell'art. 13 Cost.: l'una garantendo alla persona un certo àmbito spaziale, l'altra garantendo una delle forma più dirette di collegamento della persona con il mondo esterno. Si veda anche A. PACE, *Art. 15*, in A. BRANCA (a cura di), *Commentario alla costituzione. Rapporti civili*, Bologna, 1975, 80 ss., il quale dà atto dell'originaria intenzione del legislatore costituente di introdurre una disciplina unitaria dei tre aspetti inviolabili della persona umana. La successiva scelta di prevedere distinte norme sarebbe tuttavia ispirata a intenti garantistici: quanto alla libertà di domicilio, si possono così tutelare anche luoghi non destinati all'abitazione, quanto alla libertà di comunicazione, si esclude in tal modo che questo diritto possa subire limitazioni legittime da parte di autorità pubbliche diverse da quella giudiziaria.

essi non assurgono a rango di diritti assoluti, ma sono suscettibili di bilanciamento con altre garanzie costituzionalmente imposte[50].

La libertà personale, nata come garanzia dell'*habeas corpus* e, quindi, inizialmente concepita come assenza di coercizioni fisiche ha, in realtà, una dimensione più ampia poiché coinvolge anche la libertà morale, a condizione che il provvedimento che ne consente la limitazione non provochi una degradazione giuridica, ossia *una menomazione o mortificazione della dignità o del prestigio della persona,* [tale] *da poter essere equiparata a quell'assoggettamento all'altrui potere in cui si concreta la violazione del principio dell'habeas corpus*[51].

Essa, viene in particolare concepita come pretesa al libero svilu ppo della persona umana, rispetto al quale la libertà fisica è strumentale: l'art. 13 Cost. sarebbe, quindi, privo di un contenuto determinato e rientra, a pieno titolo, nel novero delle fattispecie c.d. a schema variabile, pur essendo in funzione della persona umana[52].

Pertanto, per individuarne l'esatto contenuto occorre fare continuo riferimento ai valori del sistema costituzionale nel suo complesso e, in particolare, ai *Grundwerte* che informano talune libertà, cioè i valori della persona[53].

La tutela della libertà personale acquisisce così quell'elasticità necessaria a garantire protezione all'individuo di fronte all'evoluzione della società (soprattutto quella tecnologica) e alla nascita di nuove forme di limitazione.

Il riferimento rileva poiché coinvolge anche un profilo particolare connesso al processo: esso si dimostra, infatti, appropriato in materia di prove atipiche la cui legittimazione ad operare nel processo è consentita soltanto a condizione che non pregiudichino la *libertà morale* della persona (art. 189 c.p.p.).

Nel verificare se un mezzo di ricerca della prova, non disciplinato dalla legge, limiti o meno la libertà di autodeterminazione, occorre, invero, fare riferimento alla libertà personale nella sua più ampia accezione e nei suoi rapporti con altri principi costituzionali: ciò soprattutto considerando che gli strumenti di indagine che *sfruttano* le innovazioni tecnologiche in campo scientifico e informatico possono conculcare la libertà personale, magari in modo meno evidente, ma comunque altrettanto insidioso rispetto alla privazione della libertà fisica.

---

[50] A. BALDASSARRE, *Diritti della persona e valori costituzionali*, Torino, 1997, 275.

[51] Corte cost., 31 maggio 1995, n. 210, in *Dir. proc. pen..*, 1996, 703.

[52] A. BARBERA, *I principi costituzionali della libertà personale*, Milano, 1967, 32 ss.; *passim*; P. BARILE, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984,196.

[53] *Ibidem*, 48.

Si pensi, ad esempio, al pedinamento satellitare che, permettendo di seguire costantemente gli spostamenti dell'individuo nello spazio, si traduce in una forma di controllo pregnante e, quindi, di limitazione della libertà personale[54].
Nel sistema delle libertà fondamentali assume rilievo anche la libertà domiciliare intesa nella sua duplice dimensione: come proiezione spaziale della persona, cioè come sfera di estrinsecazione della propria personalità e come luogo nel quale è garantito il diritto alla riservatezza[55].
La garanzia, in questo caso, non coinvolge la proprietà o altro diritto reale, ma si polarizza sul rapporto persona-ambiente, ossia *la persona riflessa in una certa sfera spaziale volta a preservare il carattere intimo, domestico, o quanto meno privato di determinati comportamenti soggettivi*[56].
Tuttavia, essa non va confusa con il diritto alla riservatezza[57], poichè, da un lato, non tutti i luoghi in cui si manifesta la personalità dell'individuo rientrano nell'ambito di applicazione dell'art. 14 Cost.; dall'altro, il particolare rapporto che si instaura tra la persona e il domicilio fa sì che esso venga tutelato anche se questa è assente (cosa che non accade per altri luoghi riservati).
Ciò che distingue il domicilio dai luoghi riservati è la *stabilità* della relazione tra la persona e il luogo, che fa ad esso acquistare autonomia rispetto alla persona titolare del diritto.
E, la differenza non è di poco conto poiché si riverbera anche in ambito processuale: le intromissioni nel domicilio devono rispettare, per espressa previsione costituzionale, le garanzie previste per la limitazione della libertà personale, mentre per quelle nei luoghi riservati - tutelati dall'art. 2 Cost. - sarebbe sufficiente un provvedimento motivato del pubblico ministero.
Allora diventa dirimente stabilire l'esatto significato da attribuire alla nozione di domicilio poiché è, ormai, notorio, che nell'ordinamento vigente non esi-

---

[54] Il tema è stato approfondito con riferimento alla tutela della privacy, da V. FANCHIOTTI, *U.S., v. Jones: una soluzione tradizionalista per il futuro della privacy?*, in *Dir. pen. proc*, 2012, 381.
[55] La tutela del domicilio è inoltre strumentale all'esercizio di altre libertà costituzionali: riunione (art. 17 Cost.), associazione (art. 18 Cost.), culto (art. 19 Cost.), insegnamento (art. 33 Cost.), iniziativa economica (art. 41 Cost.), organizzazione politica e sindacale (artt. 49 e 39 Cost.) possono svolgersi all'interno dell'area tutelata dall'art. 14 Cost. P. BARILE, E. CHELI, voce *Domicilio (libertà di)*, in *Enc. dir.*, vol. XIII, Milano, 1964, 859.
[56] *Ibidem*, 861. Si veda anche G. AMATO, *Art. 14*, in A. BRANCA (a cura di), *Commentario alla costituzione. Rapporti civili*, Bologna, 1975, 54 ss.; Corte cost., 24 aprile 2002, n. 135, in *Gius. cost.*, 2002, 1062 ss., con osservazioni di F. CAPRIOLI, *Riprese visive nel domicilio e intercettazioni «perimmagini»*; Corte cost., 7 maggio 2008, n. 149, in *Gius. cost.*, 2008, 1832 ss., con osservazioni di F. CAPRIOLI, *Nuovamente al vaglio della Corte costituzionale l'uso degli strumenti investigativi diripresa visiva*.
[57] Cass. sez. un., 28 marzo 2006, n. 26795, con nota di M. L. DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni Unite*, e di F. RUGGIERI, *Riprese visive e inammissibilità della prova*, in *Cass. pen.,* 2006, 3937 e A. CAMON, *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento ed alcuni dubbi nuovi*, in *Riv. it. dir. proc. pen.,* 2006, 1550.

ste una nozione unitaria, essendo molteplici i significati, ciascuno dei quali elaborato nell'ambito di un diverso settore normativo.
L'interrogativo che si pone coinvolge la latitudine dell'art. 14 Cost. e, cioè, se esso contempli un rinvio espresso alla nozione di domicilio elaborata nel diritto penale ovvero si riferisca ad una sfera di interessi più ampia di quella tutelata dalla norma penale[58].
Sulla questione, vi sono state differenti opzioni interpretative: da un lato, è stato messo in risalto che l'art. 14 Cost. farebbe sì rinvio alla norma penale, ma non si tratterebbe di un rinvio formale ad una fonte extra-costituzionale, ma di un rinvio recettizio, o presupposizione.
In questo caso, oggetto di tutela sarebbero l'abitazione, i luoghi di privata dimora e le loro pertinenze (art. 614 c.p.).
Una conferma di questa impostazione può rinvenirsi nel fatto che la tutela costituzionale, identificandosi nell'esistenza di un collegamento necessario e indefettibile tra domicilio e persona, viene a coincidere con la *ratio* ispiratrice della tutela penale, che correttamente colloca il delitto di violazione di domicilio tra i delitti contro la libertà individuale[59].
Dall'altro lato, viceversa, il concetto di domicilio è stato agganciato alla nozione penalistica e, pur non esaurendosi in essa, finisce per ricomprendere qualunque luogo di cui si disponga a titolo privato, anche se non si tratta di privata dimora[60].
Sul versante processuale, allora, la tendenza è quella di ampliare il concetto di domicilio in funzione della tutela penale e di circoscriverlo quando, invece, l'ambito domiciliare rappresenta un limite allo svolgimento delle indagini[61].
La questione dell'ampiezza della nozione costituzionale di domicilio si è avvertita sin dagli anni 90 anche nello specifico segmento della criminalità informatica.
Infatti, con la legge n. 547 del 23 dicembre 1993, che ha introdotto nel codice penale le fattispecie di accesso abusivo ad un sistema informatico o telematico

[58] Non sono mancati tentativi di elaborare un'autonoma nozione costituzionale di domicilio, in base all'argomento che non sarebbe corretto desumere da fattispecie particolari o extra-costituzionali l'oggetto e il contenuto di una nozione posta nella norma costituzionale. Si veda G. MOTZO, *Contenuto ed estensione della libertà domiciliare*, in *Riv. dir. proc.*, 1954, 507.
[59] In questi termini, v. P. BARILE, E. CHELI, *voce Domicilio*, cit., 859.
[60] In questo senso, in giurisprudenza, v., Cass., Sez. IV, 16 marzo 2000, n. 7063, in *Mass. Uff.*, n. 217688, secondo cui la nozione di domicilio accolta dall'art. 14 Cost. è diversa e più ampia di quella prevista dall'art. 614 c.p., finendo per coprire tutti i luoghi, siano o meno di dimora, in cui può aver luogo il conflitto di interessi che essa regola.
[61] Si veda a tal proposito la ricostruzione fatta da Cass. sez. un., 31 ottobre 2001, n. 42792, in *Cass pen*, 2002, 944.

(art. 615 *ter*) e di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater*), il legislatore ha inteso tutelare i sistemi informatici e telematici quali espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 Cost. e penalmente tutelata nei suoi aspetti essenziali dagli articoli 614 e 615 del codice penale[62].
Tuttavia, il parallelismo con il domicilio coinvolge solo parzialmente il contenuto dell'interesse all'esclusione di terzi da determinate sfere di disponibilità e rispetto, create e rese fruibili dalla tecnologia informatica[63].
Questa tensione è stata colta anche dalla giurisprudenza di legittimità, che non ha mancato di riconoscere come il codice penale tuteli il c.d. domicilio informatico quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona per cui ad esso si estende la tutela della riservatezza della sfera individuale, quale bene costituzionalmente protetto[64].
A questo punto mutano i termini del ragionamento e l'attenzione si sposta sul concetto di riservatezza, ma non per circoscrivere una distinzione rispetto al domicilio quanto a copertura costituzionale circa limiti e presupposti di ingerenza da parte degli investigatori (come hanno chiarito le Sezioni unite in materia di videoriprese)[65], bensì per sottolineare l'esistenza di un diverso bene giuridico tutelato: la riservatezza informatica[66].
La garanzia nasce come espansione del domicilio per acquistare autonomia in un ambito, quello digitale, in cui non ci sono confini e non ci sono luoghi fisici che possano riflettere il carattere privato o riservato delle attività che ivi si svolgano o di ciò che vi sia custodito.
Il nucleo essenziale del problema riguarda, allora, l'esatta individuazione della fonte del diritto alla riservatezza informatica, che è cosa ben distinta dal diritto inerente la riservatezza *tout court*.

---

[62] Così, la Relazione ministeriale al disegno di legge, 9. Sul punto, si veda L. PICOTTI, *Sistematicadei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, cit., 80.
[63] Testualmente, L. PICOTTI, *Sistematica dei reati informatici*, cit., 80.
[64] Cass., Sez. V, 26 ottobre 2012, n. 42021, *inedita.*
[65] Cfr., Cass. sez. un., 28 marzo 2006, n. 26795, cit. *Conf.*, di recente, Id., Sez. V, 17 novembre 2015, n. 11419, in *Mass. Uff.,* n. 266372.
[66] Cfr., L. PICOTTI, S*istematica dei reati informatici*, cit., 87; Id., *I diritti fondamentali nell'uso edabuso dei social network. Aspetti penali*, in *Giur. mer*, 2012, 2532; R. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, in *www.penalecontemporaneo.it;* Id. *Verso una rivalutazione dell'art. 615* ter *c.p.?,* in *Riv. trim. dir. pen. cont*, 2012, n. 2, 126; Id., *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di "domicilio informatico" e lo jus excludendi alios*, in *Dir. pen. proc.*, 2005, 81.

La riflessione intorno alle c.d. nuove dimensioni della *privacy* nell'ordinamento italiano ha visto impegnata la dottrina civilistica, costituzionalistica e penalistica dal momento che l'esigenza di tutela dei propri dati e informazioni, resa ancora più urgente dalle potenzialità di *Internet*, pervade trasversalmente diversi settori del diritto.
Il processo penale si alimenta di dati e di informazioni relative a persone identificate o identificabili e può, senz'altro, essere considerato un'ipotesi di trattamento di dati personali.
Esso, tuttavia, sfugge alle principali regole generali fissate dal codice della *privacy* – soprattutto a quelle relative ai diritti dell'interessato - in quanto strumentale al perseguimento di esigenze di giustizia (art. 47 codice *privacy*).
Tuttavia, il diritto all'autodeterminazione sui propri dati personali (sancito dall'art. 1 codice *privacy*) avendo rango fondamentale si impone come limite alle attività investigative.
La fonte di tutela costituzionale si individua nelle stesse norme a cui si riconduce il diritto alla riservatezza: il riferimento è all'art. 2 Cost. (clausola aperta), all'art. 3 Cost. (clausola generale della dignità umana), all'art. 21 Cost. (letto in negativo come libertà di non manifestare il proprio pensiero) e agli artt. 13, 14, 15 Cost. (da interpretare in modo estensivo)[67].
Queste norme, però, hanno un ambito operativo solo riflesso, mentre il diritto all'autodeterminazione informativa rientra direttamente nell'alveo delle tutele previste dall'art. 8 CEDU e dall'art. 8 della Carta dei Diritti Fondamen-

[67] Sicuramente suggestiva è la tesi che riconduce l'autodeterminazione all'art. 13 Cost. inteso come «libertà informatica» o *habeas data*. Sostiene infatti S. RODOTÀ, *Libertà personale. Vecchi e nuovinemici*, in M. BOVERO(a cura di), *Quale libertà. Dizionario minimo contro i falsi liberali*, Roma-Bari, 2004, 52, che la libertà personale non è difesa soltanto attraverso il diritto di essere lasciato solo, secondo la definizione che racchiude la più antica essenza della *privacy* e che si concreta nel potere di impedire la circolazione dei dati personali. Diviene un potere di controllo sull'esterno, sia per mantenere l'integrità di sé seguendo in ogni momento i dati diffusi nell'ambiente, sia per impedire la violazione della propria sfera privata attraverso informazioni non gradite. Il controllo sulle informazioni in entrata, strutturato in un più generale diritto di non sapere», diventa un momento caratterizzante della nuova definizione della *privacy* e incarna quel momento di intangibilità del corpo e di divieto di sue invasioni che appartiene alla più antica tradizione dell'*habeas corpus*». Questa soluzione avrebbe, tuttavia, delle conseguenze ingovernabili se calata nel processo penale. L'art. 13 Cost. prevede infatti garanzie molto rigorose, in considerazione del bene protetto che, se applicate a tutte le ipotesi in cui si apprendono dati personali attraverso mezzi di ricerca della prova, condurrebbero alla paralisi del processo. «Per qualsiasi operazione di reperimento, raccolta, elaborazione di informazioni riguardanti persone determinate dovrebbe intervenire un provvedimento autorizzativo del magistrato o una sua successiva convalida, attestante la ricorrenza di una situazione di eccezionale necessità ed urgenza che non gli abbia consentito d'intervenire personalmente. S. CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinatecostituzionali*, in D. NEGRI (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, 23.

tali dell'Unione Europea, ove è espressamente riconosciuta la tutela dei dati personali.
Ad ogni modo, anche se le nuove dimensioni della *privacy* non riguardano solo una specifica esigenza di controllo sulla circolazione dei dati personali, si avverte la necessità di riaffermare l'esistenza di quella sfera di riservatezza, i cui classici confini, legati agli spazi fisici e al tipo di informazioni che si vuole sottrarre alla conoscenza altrui, sfumano e si dissolvono[68].
A tal proposito illuminanti sono le riflessioni sostenute in relazione al bene giuridico tutelato da alcune delle nuove norme in materia di criminalità informatica (artt. 615 *ter*, 615 *quater*, 617 *quater*, 617 *quinquies*, 617 *sexies* c.p.): con il termine *dati informatici* ci si riferisce ad una pluralità di informazioni, di diversa natura, in grado di circolare con grande facilità e rapidità, duplicabili su più supporti, privi di una dimensione fisica[69].
In quest'ottica, ben si comprende, allora, come sia superata la distinzione tra dati intimi e dati sociali, tra informazioni segrete e informazioni riservate.
Un dato apparentemente innocuo, collegato ad altri dati altrettanto apparentemente innocui può, in realtà, rivelare aspetti della vita di una persona, che si desiderano sottrarre alla conoscenza altrui.
Si arriva, in questo modo, a teorizzare un nuovo bene giuridico meritevole di tutela, la *riservatezza informatica*, il cui *dna* si rinviene nell' interesse al godimento e al controllo esclusivo sia di determinati dati e informazioni, che dei relativi mezzi e procedimenti informatici e telematici di trattamento, che pur configurandosi sempre quale diritto di escludere i terzi non legittimati dal corrispondente accesso e utilizzo prescinde, in tutto o in parte, dai tradizionali limiti e presupposti dei concetti civilistici di proprietà o possesso, ovvero dalle

[68] Sostiene S. RODOTÀ, *Il diritto*, cit., 319, che nella dimensione tecnologica l'identità personale sembra dilatarsi, *disperdersi*, sino a diventare *inconoscibile* da parte dello stesso interessato. Infatti, le informazioni riguardanti una persona sono contenute in diverse banche dati, ciascuna delle quali restituisce soltanto una parte o un frammento dell'identità complessiva. Talvolta addirittura lo stesso interessato non sa dove siano dislocati i propri dati personali. Si tratta quindi di apprestare idonee forme di tutela di questa identità esterna, frutto di un'operazione nella quale sono gli altri a giocare un ruolo decisivo, con la presenza continua di elaborazione e controllo.
[69] L. PICOTTI, *Sistematica dei reati informatici*, cit., 53, distingue infatti tre diverse categorie di reati informatici a seconda dei beni giuridici tutelati (e delle modalità di aggressione). Vi sono innanzitutto fattispecie poste a tutela di beni giuridici tradizionali, offesi da nuove modalità o nuovi mezzi di aggressione, quale la frode informatica. In secondo luogo, «offese a beni giuridici analoghi a quelli tradizionali, in cui la diversità dei nuovi oggetti "passivi" su cui cadono le condotte tipiche, rispetto a quelli prima considerati dall'ordinamento, si riflettono anche sulla fisionomia dei corrispondenti beni protetti», come le falsità informatiche. «Infine, vi sono fattispecie in cui gli stessi beni giuridici offesi appaiono radicalmente nuovi perché sorti solo con lo sviluppo e la diffusione delle nuove tecnologie dell'informazione». È il caso degli artt. 615 *ter*, 615 *quater*, 617 *quater*, 617 *quinquies*, 617 *sexies* c.p.

condizioni che fondano la rilevanza giuridica del segreto o della riservatezza personale in genere[70].

La matrice ontologica del nuovo diritto è pur sempre l'esigenza di riservatezza del titolare dello *ius excludendi alios*, ma essa si spinge oltre la dimensione originaria della *privacy* e della tutela del domicilio, pur nella sua accezione di domicilio informatico[71].

La condivisibile intuizione consiste nel riconoscere che l'interesse dell'utilizzatore di sistemi informatici e telematici è quello alla tutela dei propri dati, a prescindere dal luogo in cui si trovano, o dal mezzo di comunicazione prescelto.

Tale affermazione è ben esemplificata attraverso il ricorso alla teoria c.d. assiomatica (anziché concentrica) delle sfere di tutela della vita privata secondo la quale all'interno di un sistema informatico o telematico non ha più senso distinguere tra sfera individuale e sfera privata, ma occorre prendere atto dell'esistenza di *spazi virtuali di manifestazione della personalità*, che coincidono con l'interesse sostanziale alla protezione di informazioni riservate e al loro controllo nello svolgimento di rapporti giuridici e personali *online* o in altri spazi informatici[72].

In questo contesto, è evidente che la tutela del domicilio, della segretezza delle comunicazioni ma anche della riservatezza tradizionalmente intensa, non è sufficiente.

La necessità è, quindi, quella di individuare l'esatto riferimento costituzionale al fine di stabilire i presupposti per una legittima limitazione di tale diritto da parte dell'autorità inquirente: si tratta, invero, pur sempre di un diritto soggetto al bilanciamento con contrapposti interessi ed esigenze.

La risposta sembra insita in una semplice riflessione: i principi sono destinati a coesistere con altri principi, anche se in conflitto, e ciò vale anche per quelli

---

[70] R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona. Aspetti di diritto penale sostanziale*, in *Riv. tirm. dir. pen. cont.*, 2009, 705. Si è già sottolineato come in origine, anche in base al tenore della relazione alla legge 574 del 1993 che considerava i sistemi informatici o telematici un' espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli art. 614 e 615 c.p., si era individuato il bene giuridico protetto dagli artt. 615 *ter* (accesso abusivo ad un sistema informatico o telematico) e 615 *quater* (detenzione e diffusione abusiva di codici d'accesso a sistemi informatici o telematici) nel c.d. domicilio informatico.

[71] V., R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona. Aspetti di diritto penale sostanziale*, cit., 704.

[72] R. FLOR, *Phishing, identitytheft e identityabuse. Le prospettive applicative deldiritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, 899.

concernenti i diritti inviolabili a cui è riservato uno spazio di assoluta inattaccabilità da parte dello Stato ma, al di fuori di quello spazio, la loro tutela può essere compressa in favore di altri principi che esigono di essere attuati[73].
Insomma, diventa dirimente, ancora una volta, l'aggancio a quanto contenuto nell'art. 8 CEDU e al suo valore nell'ordinamento interno.
La norma presenta, infatti, l'elasticità necessaria per coinvolgere anche la riservatezza informatica e, al tempo stesso, individua i presupposti per una limitazione di tale diritto fondamentale da parte dell'autorità pubblica.
Nel mondo del *Web* 2.0, delle comunicazioni globali e del *cloudcomputing*, non si può più distinguere tra sfera privata e sfera pubblica, e la stessa nozione di *privacy* muta e si arricchisce di contenuti nuovi con il trascorrere del tempo.
Da un lato, l'originario *right to be let alone* perde ogni riferimento alla realtà fisica; dall'altro, il *right to control the information aboutoneself*, acquista il significato di un diritto di controllo sui pacchetti di dati che viaggiano nel *web*.
Si è, quindi, forse ancora lontani dall'elaborazione di una costituzione informativa o di un *Information Bill of Rights*, che comprenda il diritto di cercare, ricevere e diffondere informazioni, il diritto all'autodeterminazione informativa, il diritto alla *privacy* informatica, ma sicuramente, grazie al sistema di tutela multilivello dei diritti fondamentali, è possibile offrire una protezione adeguata all'individuo nei confronti dei pericoli derivanti dalla tecnologia[74].
Non va, infatti, sottovalutata la circostanza che la Carta dei Diritti Fondamentali dell'Unione Europea riconosca rango di diritto fondamentale alla garanzia alla protezione dei propri dati personali (art. 8), distinguendolo dal più generale diritto alla vita privata (art. 7)[75].
La protezione multilivello dei c.d. diritti di *privacy* (art. 2 Cost., art. 8 CEDU e art. 117 Cost., artt. 7 e 8 CDFUE) assicura ad essi rango fondamentale nel sistema delle fonti ed impone il loro rispetto anche da parte dell'autorità giudiziaria nel condurre indagini penali.

---

[73] R. ORLANDI, *Garanzie individuali ed esigenze repressive (ragionando intorno aldiritto di difesa nei procedimenti di criminalità organizzata)*, in *Studi in ricordo di Giandomenico Pisapia,* Vol. II, Milano, 2000, 559.
[74] S. RODOTÀ, *Tecnologia e diritti*, Bologna, 1995, 107.
[75] Secondo, S. RODOTÀ, *Il diritto di avere diritti*, cit., 321, siamo di fronte a una vera reinvenzione del concetto di protezione dei dati personali, non solo perché viene esplicitamente considerato come un autonomo diritto fondamentale, ma perché si presenta come strumento indispensabile per il libero sviluppo della personalità e per definire l'insieme delle relazioni sociali. Si rafforza così la costituzionalizzazione della persona grazie a un insieme di poteri che davvero caratterizzano la cittadinanza del nuovo millennio

Ciò impone una riflessione sull'esistenza (*rectius* persistenza) di alcuni mezzi di ricerca della prova, o prassi investigative, poco rispettosi dei nuovi diritti fondamentali.

5. Segue: le ulteriori garanzie espresse dagli artt. 15 e 16 Cost. Nell'art. 15 Cost. si colloca una specifica tutela che si interfaccia con la libertà, la segretezza della corrispondenza e di ogni altra forma di comunicazione, consacrandole alla stregua di un vero e proprio diritto inviolabile: per questo, eventuali limitazioni possono avvenire solo per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.
Ictu oculi viene subito in rilievo che, diversamente da quanto contemplato dagli artt. 13 e 14 Cost., non sono previste eccezioni in cui la limitazione può essere disposta in via d'urgenza direttamente dall'autorità di pubblica sicurezza, salvo successiva convalida da parte dell'autorità giudiziaria[76].
Nel *corpus* dell'art. 15 Cost. la corrispondenza viene considerata una *species* del più ampio *genus* comunicazione che si sostanzia in uno scambio di idee o notizie tra mittente e destinatario – c.d. intersubiettività - e ciò vale a distinguerla dalla libertà di manifestazione del pensiero[77]: non sono, invece, rilevanti né i mezzi usati per la comunicazione, né l'oggetto in cui si concreti il suo contenuto[78].
Il versante è di rilievo poiché conferisce anche a questa protezione costituzionale quel carattere di elasticità che consente di non lasciare prive di tutela le nuove forme di comunicazione (tecnologica).
D'altronde, se la scelta del mezzo di comunicazione dovesse dipendere dal tipo di tutela che la costituzione riconosce, si assisterebbe ad una sostanziale violazione della libertà di comunicare e, più in generale, della libertà di autodeterminazione: per questo i messaggi di posta elettronica, le *chat* e i servizi *VoIP* rientrano, a pieno titolo, nell'ambito di tutela dell'art. 15 Cost.

---

[76] P. BARILE, E. CHELI, *voce Corrispondenza*, cit., 749.
[77] Secondo P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., 163, diversi sarebbero gli scopi degli artt. 15 e 21 Cost.: tutela della riservatezza della comunicazione tra soggetti determinati nel primo caso, diffusione del pensiero senza confini né segreti nel secondo. Infatti, mentre l'art. 15 Cost. costituisce un diritto fondamentale che completa il diritto della persona umana (libertà personale, libertà domiciliare, libertà di corrispondenza, libertà di circolare e soggiornare ovunque), l'art. 21 Cost. costituisce anch'esso un diritto individuale, ma che pone le basi della comunità politica moderna.
[78] In questi termini, P. BARILE, E. CHELI, *voce Corrispondenza*, cit., 744. *Contra*, A. PACE, *art. 15*, in A. BRANCA (a cura di), *Commentario alla costituzione. Rapporti civili*, Bologna, 1975, 82 ss., secondo cui, una volta individuata la matrice del diritto all'inviolabilità delle comunicazioni nella libertà di espressione, logica conseguenza sarebbe la sua attitudine a tutelare le sole forme espressive, riconoscibili come tali esteriormente. L'art. 15 Cost. non si estenderebbe quindi alle «comunicazioni di non pensieri», come ad esempio alla corrispondenza non epistolare.

La *ratio* sottesa alla tutela costituzionale si individua, invero, nell'interesse di chi comunica e nella segretezza della comunicazione: in altre parole, la tutela è volta ad impedire che altri percepiscano l'atto comunicativo in sé considerato. Controversa è, invece, la questione inerente un aspetto peculiare della tutela costituzionale: il riferimento è all'operatività anche verso l'interesse a mantenere riservato l'atto stesso del comunicare, ossia il fatto che una determinata comunicazione, intesa come fatto storico, sia avvenuta[79].

In particolare, ci si domanda se sia coperta dalla doppia riserva – legge/giurisdizione - anche l'acquisizione dei c.d. dati esteriori di una comunicazione, quali ad esempio, il numero chiamato, la durata, l'ubicazione, ecc.

Lo specifico profilo è stato scandagliato dalla Corte costituzionale la quale, chiamata a pronunciarsi in merito, ha affermato che l'ampiezza della tutela sottesa all'art. 15 Cost. è tale da ricomprendere nel proprio alveo anche i dati esteriori di individuazione di una determinata conversazione telefonica: si tratta di una prerogativa connaturata al diritto costituzionale che si riferisce non solo alla segretezza, ma anche alla libertà delle comunicazioni offrendo una protezione molto ampia al diritto dei singoli di intrattenere relazioni riservate[80].

Sulla *questio* anche la dottrina ha preso posizione rilevando che tra i due versanti - libertà e segretezza - è senz'altro la prima a caratterizzare la tutela costituzionale: *ergo*, la segretezza sarebbe da intendersi solo come uno strumento volto a garantire la libertà[81].

In questo modo, la libertà di comunicare viene concepita come parte necessaria di quello spazio vitale che circonda la persona e senza il quale non può svilupparsi in armonia con i postulati della dignità umana[82].

---

[79] Così, F. CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2002, 66.

[80] Corte cost., 11 marzo 1993, n. 81, in *Cass. pen.*, 1993, 2744. Conforme, Corte cost., 17 luglio 1998, n. 281, in *Gius. cost.*, 1998, 2721. Anche la Corte Europea dei Diritti dell'Uomo ha riconosciuto che l'utilizzazione come mezzo di prova dei tabulati telefonici integra un'ingerenza nella *privacy* e incide pertanto sul diritto al rispetto della vita privata, tutelato dall'art. 8 CEDU. Cfr. Corte europea dei diritti dell'uomo, *Heglas v. Czech Republic*, in *Cass. pen.*, 2007, 3947, con nota di L. DE MATTEIS. Si veda anche A. BALSAMO, A. TAMIETTI, *Le intercettazioni, tra garanzie formali esostanziali*, in A. BALSAMO, R. E. KOSTORIS (a cura di), *Giurisprudenza europea e processo penale italiano*, Torino, 2008, 464. Anche la Corte costituzionale tedesca, nell'importante sentenza sullalegge di attuazione della direttiva *data retention*, ha ritenuto che i dati c.d. esterni di una comunicazione rientrino nell'ambito di tutela dell'art. 10, comma 1 GG, che garantisce la segretezza delle comunicazioni (*Fernmeldegeheimnis*). *BVerfG*, 2 marzo 2010, *1BvR 256/08*, *1 BvR 263/08*, *1BvR 586/08*, in *www.bundesverfassungsgericht.de*. In dottrina, si veda, *ex multis*, A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005, 594 ss.

[81] In tal senso P. BARILE, *Diritti dell'uomo*, cit., 164.

[82] Corte cost., 11 marzo 1993, n. 81, cit.

Pur apprezzandone l'impostazione garantista, simile approdo interpretativo non è, però, confortato da altra parte della dottrina[83] il cui ragionamento si incentra nel fatto che gli artt. 14 e 15 Cost. assicurino, invece, il diritto dell'individuo all'inaccessibilità (o intimità) della propria sfera privata, da intendersi come diritto a coltivare la propria personalità in ambiti spirituali (la comunicazione riservata) e spaziali (il domicilio) sottratti all'ascolto e all'osservazione di estranei[84].

Dunque, l'interesse a non rendere noto che una comunicazione sia avvenuta (quando e dove), presenta maggiore affinità con il diritto alla riservatezza, inteso come interesse al controllo sulla circolazione e sull'uso delle notizie personali, del quale condividerebbe il (limitato) regime di tutela costituzionale ed esula dalla tutela che l'art. 15 Cost. accorda alla sfera privata[85].

A ben vedere, quest'ultima opzione interpretativa, pur facendo rientrare nell'orbita di tutela dell'art. 15 Cost. anche i dati esterni, non risolve il delicato problema di fondo e cioè se per la loro acquisizione sia necessario o meno un provvedimento del giudice, così come previsto per le intercettazioni[86] o se, viceversa, sia sufficiente un provvedimento del pubblico ministero[87].

La soluzione è stata offerta dal legislatore che, intervenuto a disciplinare la materia della conservazione e acquisizione dei dati di traffico telefonico con il d. lgs n. 196/2003 (c.d. codice *privacy*), dopo aver inizialmente attribuito al giudice la specifica competenza ad emettere il provvedimento acquisitivo ha, successivamente, ritenuto sufficiente un decreto del pubblico ministero da adottare ai sensi della norma contenuta nell' art. 256 c.p.p.

Quindi, la soluzione adottata risulta essere del tutto compatibile con i presidi tutelati dall'art. 15 Cost., laddove è richiesto che la limitazione del diritto ivi garantito avvenga per mezzo di un provvedimento dell'autorità giudiziaria, sia essa il giudice o il pubblico ministero[88].

In altre parole, pur essendo unico il diritto che viene in considerazione, i presupposti per l'adozione di limitazioni dello stesso variano a seconda

---

[83] Così, F. CAPRIOLI, *Colloqui riservati*, cit., 68.

[84] *Ibidem*, p. 56. Tanto è vero che, parafrasando la definizione di domicilio come proiezione spaziale della persona, autorevole dottrina penalistica ha parlato della comunicazione riservata come di una proiezione spirituale del soggetto che la pone in essere. F. BRICOLA, *Prospettive eliniti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen.*, 1967, 1120.

[85] F. CAPRIOLI, *Colloqui riservati*, cit., 70.

[86] In questo senso, Cass. sez. un., 13 luglio 1998, n. 21, in *Gius. pen.*, 1999, III, c. 614.

[87] Così, allineandosi all'orientamento della Corte costituzionale che aveva escluso l'applicabilità della disciplina delle intercettazioni. Cass. sez. un., 23 febbraio 2000, n. 6, in *Giur. it*, 2001, 1707.

[88] La stessa Corte costituzionale, nella sentenza n. 81 del 1993 cit., aveva precisato che spettava al legislatore l'individuazione dell'autorità giudiziaria (giudice o pubblico ministero) competente ad emanare il provvedimento acquisitivo dei tabulati telefonici.

dell'intensità dell'intromissione nella sfera privata: il tutto, però, nel rispetto del dettato costituzionale[89].

L'utilizzo di nuove tecnologie per condurre classiche attività di indagine impone di prendere in considerazione anche diritti di libertà che, a prima vista, poco hanno a che vedere con i mezzi di ricerca della prova.

Il riferimento è, questa volta, all'uso del *gps* per seguire e monitorare gli spostamenti della persona nello spazio e, quindi, all'art. 16 Cost. che garantisce la libertà di circolazione e soggiorno.

Anche questo diritto è strettamente connesso alla libertà personale al punto da far nascere una *querelle* tra coloro che ne negano l'autonomia rispetto alla sfera di tutela offerta dall'art. 13 Cost.[90]e coloro che, viceversa, partendo dal dato costituzionale, riconoscono che si tratta di due libertà distinte, ancorché interfacciabili.

L'impostazione fa leva sul fatto che la libertà tutelata dall'art. 16 Cost. riguarderebbe un momento cronologicamente successivo a quello della libertà personale, presupponendola e sviluppandola[91]: entrambe, però, sarebbero da intendersi come espressione della più ampia libertà di autodeterminazione della persona[92].

Dunque, l'operatività della tutela sottesa all'art. 16 Cost sarebbe limitata e non avrebbe ad oggetto tutte le restrizioni alla libertà di circolazione e soggiorno, ma riguarderebbe soltanto quelle che non "*toccano*", direttamente ed immediatamente, la persona in taluno dei suoi attributi essenziali, come la sua dignità sociale e la sua personalità morale[93].

In altre parole, l'art. 16 Cost. avrebbe la funzione di tutelare l'individuo da forme di controllo dei suoi movimenti che non raggiungono la soglia della restrizione della libertà personale, ma che sono, comunque, in grado di comprimere la sua libertà di autodeterminazione, fungendo da remora a determinati spostamenti[94].

---

[89] Similmente a quanto afferma la Corte di Strasburgo con riferimento all'art. 8 CEDU. *Contra*, F. CAPRIOLI, *Colloqui riservati*, cit., 71.

[90] Ampiamente V. CRISAFULLI, *Libertà personale, costituzione e passaporti*, in *questa rivista*, 1955, 117; M. GALIZIA, *La libertà di circolazione e soggiorno (dall'Unificazione alla Costituzione repubblicana)*, in P. BARILE (a cura di), *La pubblica sicurezza*, Milano, 1967, 545; U. DE SIERVO, *voce Soggiorno, circolazione, emigrazione (Libertà di)*, in *Nuov. dig. it.*, vol. XVII, Torino, 1970, 822.

[91] P. BARILE, *Diritti dell'uomo*, cit., 172. Secondo G. VASSALLI, *La libertà personale*, cit., 405, ne deriverebbe un concetto unitario di libertà personale, intesa come «l'interesse di ogni individuo a non essere in nessun modo turbato nella propria attività esterna in sé e per sé considerata». La questione dell'ambito di applicazione delle due norme costituzionali, si era posta con riferimento alle misure di prevenzione.

[92] In argomento, diffusamente, cfr., S. GALEOTTI, *La libertà personale*, Milano, 1953, 12.

[93] A. BARBERA, *I principi costituzionali*, cit., 200.

[94] A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, cit., 633.

Così concepito, il diritto alla libertà di circolazione, si arricchirebbe di una nuova componente e cioè il diritto a non essere localizzati, il che comporta evidenti riflessi anche in tema di indagini ove il confine tra limitazione della libertà personale e restrizione della libertà di circolazione è molto labile[95].
Infatti, da tempo si è dibattuto sulla distinzione tra la libertà di locomozione, intesa come possibilità di disporre dei propri movimenti e, quindi, come una delle facoltà in cui si esplica il godimento della libertà personale, tutelata dall'art. 13 Cost. e la libertà di circolazione e soggiorno in senso stretto che, invece, costituisce una forma di manifestazione della libertà personale in merito alla possibilità di spostarsi da una località all'altra[96].
Nell'alveo di queste coordinate interpretative il c.d. pedinamento *gps* costituirebbe, sicuramente, una limitazione della libertà personale con evidenti risvolti in relazione ai presupposti di adozione di simili strumenti investigativi: differenti, invero, a seconda che l'attività di indagine si iscriva nell'art. 13 ovvero nell'art. 16 Cost.[97]
In una famosa sentenza della Corte suprema dell'Oregon del 1988 si sono "*mappati*" gli effetti che alcuni strumenti di controllo (il riferimento è al *trackingGPS* o alle videoriprese) possono avere sulla libertà di autodeterminazione della persona, nella sua duplice espressione di libertà morale e libertà di circolazione e movimento: in essa si è sottolineato che ogni strumento che consenta alla polizia di localizzare rapidamente una persona o un oggetto per un periodo prolungato, costituisce una significativa limitazione della libertà personale, intesa come libertà dal controllo – *freedom fromscrutiny*-[98].
Addirittura, la libertà di autodeterminazione sarebbe messa in crisi in misura uguale, se non maggiore, dalla semplice minaccia del controllo rispetto al controllo effettivo.
E' sulla base di queste premesse che in fondo si è, di fatto, teorizzata l'esistenza di un *constitutional right to freedom from technologicallyadvancedscrutiny*, ricavabile dall'art. 1, par. 9 della Costituzione dello Stato dell'Oregon, che al pari del IV Emendamento alla Costituzione americana, tutela la libertà personale degli individui[99].

---

[95] *Ibidim*, 633.
[96] G. VASSALLI, *La libertà personale*, cit., 384.
[97] In tema, v., L. FILIPPI, *Il GPS è una prova incostituzionale? Domanda provocatoria, ma non troppo, dopo la sentenza* Jones *della Corte Suprema* U.S.A., in q*uesta rivista*, 2012, 309.
[98] *State v. Campell*, 759 P. 2d 1040, 1048-1049 (Or. 1988). In merito si veda D. J. GLANCY, *Privacy on the Open Road, 30 Ohio N. U. L. Rev. 295 (329).*
[99] L. FILIPPI, *Il GPS è una prova incostituzionale? Domanda provocatoria, ma non troppo, dopo lasentenza* Jones *della Corte Suprema* U.S.A., cit. 310.

La pronuncia della Corte federale è servita da monito per i giudici italiani i quali, nel tracciare le coordinate di riferimento del perimetro nel cui ambito l'attività di monitoraggio elettronico dovrebbe estrinsecarsi, hanno precisato che il controllo a distanza con *gps* non costituisce un'intercettazione (il che è corretto), ma si sostanzia in una modalità tecnologicamente caratterizzata di pedinamento che rientra nel novero delle prove atipiche - utilizzabili dall'organo inquirente – "*sganciate*" dai formalismi richiesti dagli artt. 266 e ss. c.p.p.[100]

Ciò nonostante, anche per questo tipo di strumento il superamento dell' "*esame*" dell'art. 189 c.p.p. non risolve la questione relativa alla legittimità e, quindi, alla conseguente utilizzabilità dei dati e delle informazioni con esso ottenibili dall'organo inquirente: anche in questo caso, infatti, l'esigenza è quella di verificare la eventuale esistenza di limiti connessi alla necessità di tutelare valori costituzionali in conflitto con l'esigenza di accertamento dei reati che giustifica l'utilizzo dello strumento investigativo.

La disciplina costituzionale di riferimento assume un triplice rilievo, fungendo, al contempo, da limite ermeneutico, da parametro di legittimità e, sia pure in modo più controverso, da fonte di *exclusionaryrules*[101].

In questo caso, allora, l'analisi della eventuale compressione di diritti fondamentali dovuta al pedinamento elettronico necessita di una premessa di natura tecnica, che chiarisca la differenza esistente tra il rilevamento satellitare vero e proprio e l' attività ad esso propedeutica di tipo preparatorio.

Lo strumento investigativo consiste nel monitoraggio in tempo reale del segnale satellitare contenente le informazioni relative alla posizione ed allo spostamento del soggetto: viceversa, l'attività ad esso propedeutica si sostanzia nella materiale intrusione all'interno del mezzo da controllare al fine di installare la stazione che riceve il segnale.

Dunque, se per il rilevamento satellitare *tout court* non sembrano sussistere particolari problemi (come anticipato, da escludere, l'incidenza dell'art. 15 Cost. a causa della inidoneità del mezzo *de quo* ad interferire con la libertà e la segretezza delle comunicazioni)[102], parimenti sembra fuorviante immaginare una lesione della libertà psico-fisica del soggetto monitorato, assolutamente ignaro del controllo subito[103].

Ma ciò non è sufficiente a mettere la parola fine alla questione: occorre scandagliare il versante inerente la compatibilità dello strumento investigativo ri-

[100] Cfr., per tutte, Cass. Sez. IV, 27 novembre 2011, n. 48279, in *Mass. Uff.,* n. 253953.
[101] Così, C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007, 245,
[102] Cass., Sez. VI, 11 aprile 2008, n. 17265, in *Mass. Uff.,* n. 239628.
[103] C. MARINELLI, *Intercettazioni processuali*, cit., 262.

spetto al diritto alla riservatezza, recepito a livello costituzionale dall'art. 2 Cost.

La soluzione è contesa tra chi ritiene che il diritto alla *privacy*, estendendosi ad aspetti della vita privata quali i luoghi frequentati o la circolazione dei singoli sul territorio, non potrebbe ritenersi sufficientemente tutelato in un sistema che ammetta una localizzazione satellitare senza limiti[104]e chi, invece, sostiene che la genericità dell'art. 2 Cost. comporta il necessario ricorso ad altre disposizioni costituzionali al fine di individuare la esatta area di copertura del diritto alla riservatezza in modo che l'eventuale compressione del diritto alla *privacy* - svincolata da un contesto domiciliare o comunicativo -, non comporti alcuna ipotesi di prova incostituzionale[105].

Tra l'altro, non va trascurato che la localizzazione satellitare presuppone, comunque, un'attività di intrusione all'interno dell'autovettura del soggetto da monitorare al fine di installare la stazione ricevente il segnale *gps* proveniente dai satelliti[106].

E qui la questione non è di poco conto perché coinvolge un bene (l'abitacolo dell'autovettura) che rientra nel novero delle tutele protette dall'art. 14 Cost., in quanto si tratta, pur sempre, di un ambito spaziale isolato rispetto all'esterno destinato allo svolgimento di attività inerenti la vita privata e caratterizzato da uno *ius excludendi alios* in capo al titolare del mezzo[107]. Sullo specifico profilo è stato posto in risalto che la legittimità dell'intervento intrusivo, finalizzato alla predisposizione del ricevitore *gps*, necessita di una previsione legislativa in ordine ai "*casi e ai modi*" in cui può avvenire.

Soluzione, quest'ultima, non condivisa dalla giurisprudenza che, viceversa, tende ad escludere che l'abitacolo dell'autoveicolo possa qualificarsi come domicilio rilevante ai fini dell'art. 14 Cost.: essendo un mezzo di trasporto l'autovettura difetta di quelle caratteristiche tipiche dei luoghi di privata dimo-

---

[104] L.G. VELANI, *Nuove tecnologie e prova penale: il sistema di individuazione satellitare g.p.s*, in *Giur. it.,* 2003, 2375, il quale, a ragionar diversamente, avverte anche una potenziale violazione dell'art. 3 Cost., a causa della irragionevole disparità di trattamento tra mezzi di ricerca della prova nominati, per i quali è previsto dal codice di rito il controllo giurisdizionale, e strumenti atipici comunque incidenti, quantomeno, sulla riservatezza

[105] Così, C. MARINELLI, *Intercettazioni processuali*, cit., 247.

[106] Tecnicamente, tale intrusione può essere fatta in due modi: intervenendo dall'esterno e collocando il dispositivo direttamente alla batteria contenuta nel vano motore del veicolo; inserendo la ricevente all'interno dell'abitacolo, opportunamente occultata, onde evitare il rischio di essere scoperti. Cfr., A. SERRANI, *Sorveglianza satellitare GPS: un'attività investigativa ancora in cerca di garanzie*, in *Aech. pen.*, 2013, 3.

[107] Cfr. G. BORRELLI, *Riprese filmate nel bagno di un pubblico esercizio e garanzie costituzionali*, in *Cass. pen.*, 2001, 2453; C. FANUELE, *Il concetto di privata dimora ai fini delle intercettazioni ambientali*, in *Cass. pen.,* 2001, 2746.

ra capaci di consentire l'espletamento, in condizioni di riservatezza, delle più elementari funzioni umane[108]. Si esclude, quindi, che per l'attività in oggetto sia necessaria una specifica legge di copertura né, tantomeno, occorre la previa autorizzazione dell'autorità giudiziaria.
Sarebbe opportuno un intervento legislativo in *subiecta materia* volto ad introdurre una disciplina specifica capace di realizzare quel tanto reclamato equo bilanciamento tra opposte esigenze: accertamento penale, da un lato, e tutela dei diritti individuali coinvolti in tale accertamento, dall'altro.
Infatti, sulla scia del progresso tecnologico foriero di mezzi di indagine sempre più penetranti e invasivi, la supplenza giurisdizionale può diventare rischiosa: ed allora, anche con riferimento al rilevamento mediante *gps,* sarebbe opportuno un intervento legislativo *ad hoc* attraverso il quale venissero specificate le tipologie di reato per le quali consentire (legittimandole) il monitoraggio, le modalità preparatorie ed esecutive, la riserva di giurisdizione, la forma della documentazione delle operazioni, le sanzioni processuali in ipotesi di violazione dei presupposti legittimanti l'uso dello strumento investigativo[109].

6. *La tutela Convenzionale del diritto alla vita privata.* La necessità di riconoscimento dei diritti in questo ambito, ha allertato il legislatore dei vari ordinamenti delle società moderne in cui si affermano libertà inedite ed invocano tutele diritti che sono da considerarsi inattesi: istanze egualitarie e azioni di protezione, protocolli di rappresentanza si affacciano nell'originario *pantheon* dei diritti e pretendono garanzie che ancora non sono state strutturate in modo adeguato[110].
La *privacy* si erge a paradigma di questa categoria di diritti "*liquidi*", ossia anamorfici, privi di contenuti stabili e, talvolta, derivanti da altri diritti (corrispondenza, domicilio, ecc.)[111].

---

[108] Cfr. Cass. sez. un., 31 ottobre 2001, n. 42792, in *Foro it.,* 2002, II, c. 170. In dottrina, a favore della impossibilità di ricondurre l'abitacolo dell'autoveicolo al concetto di domicilio, cfr. P. GIORDANO, *Inapplicabile garanzie dell'intercettazione al semplice monitoraggio della posizione*, in *Guida. dir.*, 2002, 23, 54, secondo il quale esiste una ontologica ed insuperabile differenza tra un mezzo di trasporto e una privata dimora, poiché quest'ultima echeggia una struttura abitativa stabile tendenzialmente immobiliare.
[109] Di questo avviso, fra gli altri, L. FILIPPI, *Il gps è una prova "incostituzionale"?* cit., 310.
[110] Ampiamente, A. CISTERNA, *CEDU e diritto alla privacy*, in A.A.V.V., *I principi europei del processo penale*, a cura di A. GAITO, Roma, 2016, 194.
[111] Così osservavano, T.A. AULETTA, *Riservatezzae tutela della personalità*, Milano, 1978, 27; A. CERRI, *voce riservatezza, (diritto alla), Diritto comparato*, in *Enc. giur. tr.*, XXXVII, Roma, 1991, 3; M. BONETTI, *Riservatezza, diritti dell'uomo e processo penale: aspetti problematici*, in *Ind. pen.*, 1995, 87; S. RODOTÀ, *La privacy tra individuo e collettività*, in *Pol dir.,* 1974, 551. Per una ricostruzione dell'evoluzione giurisprudenziale, cfr., G. BUTTARELLI, *Banche dati e tutela della riservatezza: la privacy e la Società*

Malgrado ciò, la lesione alla sfera soggettiva (ovvero alla *privacy*) avviene secondo modalità aggressive non agevolmente classificabili[112]: si pensi, ad esempio, all'autorizzazione che inconsapevolmente viene data accettando l'invito di *cookies* navigando su *Internet* e, quindi, consentendo di apprendere dati personali[113].

A questa morfologia dispositiva del diritto deve essere conseguenziale che la tutela giurisdizionale si manifesti con connotati di elasticità: la questione abbraccia, coinvolgendola, la giurisdizione nazionale[114] e, soprattutto, quella sovranazionale che oscilla nella ponderazione dei diritti antagonisti alla *privacy*, enucleando giudizi di valore discutibili in merito ai diritti in contesa[115].

Il continuo progresso delle tecniche di rilevamento, conservazione ed analisi dei dati personali[116], costituisce non tanto una minaccia concreta alla riservatezza personale quanto, piuttosto, il mezzo con cui aspettative e diritti raggiungono soglie di tutela un tempo impensabili[117].

---

dell'Informazione, Milano, 1997, 34 ss.; F. CARNELUTTI, *Diritto alla vita privata*, in *Riv. trim. dir. pen.*, 1955, 14; G. GIACOBBE, *voce riservatezza (diritto alla)*, in *Enc. dir.,* XI, Milano, 1989, 1253; F. MODUGNO, *"I nuovi diritti" nella giurisprudenza costituzionale*, Torino, 1995, 25 ss.

[112] In argomento, V. FROSINI, *Teoria e tecnica dei diritti umani: i diritti umani nella società tecnologica*, Napoli, 1993, 37; F. GALGANO, *La globalizzazione nello specchio del diritto*, Milano, 2005, 141.

[113] M. MARCELLI, *Internet fra canale di comunicazione politica e strumenti di controllo. Profili di diritto internazionale*, in F. MARCELLI, P. MARSOCCI, M. PIETRANGELO, (a cura di), *La rete internet come spazio di partecipazione politica. Una prospettiva giuridica*, Napoli, 2015, 34; V. ZENO ZENCOVICH, *Appunti sulla disciplina costituzionale delle telecomunicazioni*, in *Dir. inform. inf.*, 1996, 93.

[114] In questi termini Cass. civ., 5 ottobre 2010, n. 18279, in *Mass. Uff.* n. 614526, secondo cui nelle controversie in cui si configura una contrapposizione tra due diritti, aventi entrambi copertura costituzionale, e cioè tra valori ugualmente protetti, va applicato il cd. criterio di "gerarchia mobile", dovendo il giudice procedere di volta in volta, ed in considerazione dello specifico "*thema decidendum*", all'individuazione dell'interesse da privilegiare a seguito di un'equilibrata comparazione tra diritti in gioco, volta ad evitare che la piena tutela di un interesse finisca per tradursi in una limitazione di quello contrapposto, capace di vanificarne o ridurne il valore contenutistico. Ne consegue che il richiamo ad opera di una parte processuale al doveroso rispetto del diritto (suo o di un terzo) alla *privacy* non può legittimare una violazione del diritto di difesa che, essendo inviolabile in ogni stato e grado del procedimento ex art. 24, comma secondo, Cost., non può incontrare nel suo esercizio ostacoli ed impedimenti nell'accertamento della verità materiale a fronte di gravi addebiti suscettibili di determinare ricadute pregiudizievoli alla controparte in termini di un irreparabile "vulnus" alla sua onorabilità e, talvolta, anche alla perdita di altri diritti fondamentali, come quello al posto di lavoro

[115] Cfr., Corte EDU, sez. IV, 12 gennaio 2016, n. 61496, in *Ilgiustlavorista.it*, 2016, con nota a cura di G. DE LUCA. Di recente, v., M. GROTTO, *La rilevanza penale del controllo datoriale attraverso gli strumenti informatici*, in *Dir. inform. inf.*, 2014, 57

[116] Per la definizione aggiornata di dati personali, v., art. 3 n. 1 Dir. (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati e o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977 GAI secondo la quale sono dati personali qualsiasi informazione riguardante una persona fisica identificata o identificabile.

[117] In argomento diffusamente, cfr., S. CIAMPI, *Principio di disponibilità e protezione dei dati personali nel*

Ma la rete è capace di "*sequestrare*" ogni identità per custodirla e restituirla, di volta in volta, rendendone evidente l'uso[118].
In questo contesto, allora, la risposta del processo avrebbe dovuto assicurare un perimetro d'azione abbastanza circoscritto agli strumenti informatici invasivi: ma è noto che ciò non sia accaduto[119] per una serie di ragioni più disparate[120].
Abbiamo visto che la disciplina che l'ordinamento interno appresta a salvaguardia del diritto alla *privacy* è, in larga parte, condizionata dall'art. 189 c.p.p. che, nel regolare la tipicità di alcune fonti di prove, ne consente l'assunzione a determinate condizioni[121]: si pensi, ad esempio, alla legittimazione del pedinamento elettronico tramite *gps*[122].
Dunque, diventa dirimente trovare il bandolo della matassa tra gli interessi in contesa: ancora una volta accertamento del reato, da un lato, e tutela della vita privata e familiare, dall'altro.
In assenza di norme specifiche, bisogna guardare alle disposizioni convenzionali per sincerarsi della legalità di attività intrusive destinate a squilibrare l'assetto probatorio del processo[123].

"terzo pilastro" dell'Unione europea, in F. PERONI, M GIALUZ, (a cura di), *Cooperazione informativa, e giustizia penale nell'Unione europea*, Torino, 2009, 34; B. PIATTO, *Il principio di proporzionalità e il trattamento dei dati personali nella lotta al terrorismo*, in *Dir. pen. proc.*, 2015, 885.

[118] Così si esprime A. CISTERNA, *CEDU e diritto alla privacy*, cit., 200.

[119] Secondo S. FURFARO, *(voce) Riservatezza*, in *Dig. pen.,* IV, Torino, 2008, 1062, l'indagine è la fase del processo che registra le contraddizioni maggiori e sollecita atteggiamenti diversi, soprattutto nel momento delle autorizzazioni e nelle verifiche delle "*invasioni della sfera privata*". In tale ambito, l'ampliamento delle possibilità di apprensione di dati offerto dallo sviluppo tecnologico e scientifico consente, sempre con maggiore facilità, la violazione di spazi coperti dalla riservatezza.

[120] Ritiene A. CISTERNA, *CEDU e diritto alla privacy*, cit., 201, che le ragioni del fallimento sono molteplici ed affondano le radici nella miscela esplosiva di fenomeni culturali, assetti ordinamentali, prescrizioni processuali ed indirizzi nomofilattici.

[121] Secondo C. ANGELONI, *Nota in tema di registrazioni fotografiche*, in *Giur. it*, 2010, 7, l'art. 189 c.p.p. non rispetta il canone della riserva di legge enunciato dall'art. 8 CEDU.

[122] Cass. sez. II, 13 febbreaio 2013, n. 21644, in *Mass. Uff.* n. 255542, secondo cui l'attività di indagine volta a seguire i movimenti di un soggetto ed a localizzarlo, controllando a distanza la sua presenza in un dato luogo in un determinato momento attraverso il sistema di rilevamento satellitare (cosiddetto *GPS*) costituisce una forma di pedinamento eseguita con strumenti tecnologici, non assimilabile in alcun modo all'attività di intercettazione prevista dagli artt. 266 e ss. c.p.p.; essa non necessita, quindi, di alcuna autorizzazione preventiva da parte del giudice per le indagini preliminari poiché, costituendo mezzo atipico di ricerca della prova, rientra nella competenza della polizia giudiziaria. In dottrina, S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. mer*, 2013, 955.

[123] La dottrina maggioritaria ritiene che la tutale sottesa all'art. 2 Cost. non sia sufficiente a tuelare la *privacy*. Cfr., T.A. AULETTA, *Riservatezza e tutela della persona, Milano*, 1978, 42; F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv.it. dir. proc. pen.*, 1967, 1091; P. CARETTI, *I diritti fondamentali*, Torino, 2002, 228; S. RODOTÀ, *La rivoluzione della dignità*, Napoli, 2013, 37.

Le previsioni normative contenute negli art. 8 CEDU e 7 e 8 CDFUE costituiscono, senz'altro, il parametro adoperato dai giudici per arginare le intrusioni nella vita privata che l'organo inquirente può realizzare[124].
Si tratta di questioni che, sicuramente, sono destinate ad interagire con il canone del giusto processo (art. 6 CEDU) per cui è inevitabile che la pretesa violazione della *privacy* nell'uso di mezzi investigativi, si riverberi e comprometta anche l'equità del processo[125].
Così, in questa delicata materia, la Corte EDU ha tracciato una *guideline* nel tentativo di far assumere carattere cogente al diritto alla *privacy* che rappresenta, a tutt'oggi, la vittima illustre dell'inerzia perdurante del legislatore.
Sono tre i profili individuati che operano in modo interconnesso e che dovrebbero costituire il parametro di riferimento delle giurisdizioni nazionali[126].
Conoscibilità della disposizione normativa da parte di tutti i cittadini, in modo che ad essa si possa conformare la propria condotta prevedendone, ragionevolmente, le conseguenze[127]; utilizzazione di un linguaggio facilmente comprensibile da parte del cittadino, in modo che sappia in quali casi e in presenza di quali presupposti è legittimato l'uso di strumenti invasivi; protezione adeguata contro gli atti arbitrari dell'organo inquirente, in modo che il cittadino possa regolare la propria condotta sapendo in quali casi è consentita l'intrusione nella sua sfera privata[128].
Queste coordinate di riferimento, la cui inosservanza determina la violazione dell'art. 8 CEDU, fondano sulla convinzione secondo la quale ogni intromissione nella vita privata rappresenta un'ingerenza nella sfera privata, anche quando di essa non si sia fatto un uso processualmente rilevante[129].
La tutela, dunque, si estende fino a coinvolgere l'acquisizione di ogni elemento relativo allo svolgimento normale delle relazioni umane.
Vista la delicatezza dei diritti coinvolti e considerato che tutte le intrusioni nella vita privata costituiscono violazione di un diritto fondamentale, queste deb-

[124] Per un approfondimento del concetto di *privacy* da parte delle Corti europee, v., G. TIBERI, *Il diritto alla protezione dei dati personali nelle Certe e nelle Corti sovranazionali (in attesa del trattato di Lisbona), I parte*, in *Cass. pen.,* 2009, 4467; Id., *Il diritto alla protezione dei dati personali nelle Certe e nelle Corti sovranazionali (in attesa del trattato di Lisbona), II parte*, in *Cass. pen,* 2010, 355.
[125] Al riguardo, F. M. MOLINARI, *L'art. 6 Cedu come parametro di effettività della tutela procedimentale e giudiziale all'interno degli Stati membri dell'Unione europea*, in *Riv. tri. dir. pen. cont.*, 2012, 267.
[126] Il riferimento è a Corte EDU, Sez. IV, 10 febbraio 2009, *caso Iordachi c. Moldavia,* in *Cass. pen.*, 2009, 4023, con nota di A. BALSAMO.
[127] Cfr., sentenza *caso Cobam c. Spagna*, 26 novembre 2006, n. 17060/02.
[128] Cfr., A. CISTERNA, *CEDU e diritto di privacy*, cit., 215.
[129] V. Corte EDU, *Kopp c. Svizzera*, 25 marzo 1998; *caso Ludi c. Svizzera*, 15 giugno 1992, 51

bono essere previste e giustificate da una legge dello Stato (art. 8 par. 2 CEDU)[130].

La norma (art. 8 par. 2 CEDU) traccia la latitudine del contenuto della legge precisando che *non può esservi ingerenza dell'autorità nell'esercizio del diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.*

Tuttavia, per non *bypassare* i limiti della necessità, la Corte EDU ha precisato che l'ingerenza, per risultare legittima, deve essere proporzionata rispetto alla giustificazione invocata[131].

Nella consapevolezza di dare concreta tutela alla nuova dimensione della *privacy* anche la Carta di Nizza (CDFUE) ha normato la materia con due differenti disposizioni che tutelano, rispettivamente, il diritto al rispetto della vita privata e familiare, del domicilio e delle comunicazioni (art. 7) e il diritto alla protezione dei dati personali (art. 8).

Si vuole dare autonoma rilevanza a quel *right to control of the information aboutone self*, già considerato componente essenziale della *privacy*.

Il dato è riscontrato dal fatto che lo stesso Trattato di Lisbona introduce una specifica azione rivolta all'Unione avente ad oggetto la tutela del diritto alla protezione dei dati personali (art. 16, comma 2 TFUE)[132].

Ai sensi dell'art. 52, comma 1 CDFUE eventuali limitazioni all'esercizio dei diritti e delle libertà devono essere attuate attraverso una specifica legge: possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. Invece, nel comma 3 è previsto che laddove la Carta contenga diritti corrispondenti a quelli garantiti dalla

---

[130] Corte Edu, 26 aprile 1979 richiamata in L. FILIPPI, *Intercettazioni telefoniche (dir. proc. pen.)*, in *Enc. dir.*, Agg., VI, Milano, 2002, 572.

[131] Ampiamente in Corte EDU, 23 settembre 1998, *McLeod c. Regno Unito*; 9 gennaio 2001, *caso Natoli c. Italia*.

[132] Tale norma, dopo aver ribadito l'esistenza di un diritto alla protezione dei dati personali, meritevole di tutela, prevede che «il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. Per un approfondimento, cfr., G. DI PAOLO, *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in *Cass. pen.*, 2010, 1985.

CEDU, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione (c.d. clausola di equivalenza).
Dunque, i *vulnus* sottesi agli articoli 7 e 8 CDFUE vanno riempiti di significato alla luce dell'art. 8 CEDU, soprattutto per quanto riguarda i presupposti di un'ingerenza legittima negli stessi da parte della pubblica autorità.
A tal proposito si segnala che, in una recente sentenza in materia di tutela dei diritti d'autore in *Internet*, la Corte di Giustizia, facendo proprie le conclusioni dell'avvocato generale, Pedro Cruz Villalòn, ha ribadito l'equivalenza tra l'art. 8 CEDU e gli artt. 7 e 8 CDFUE[133].
Il dato si riflette nell'ambito delle indagini informatiche e via *Internet*, ove il diritto alla tutela dei dati personali, quale filiazione del diritto al rispetto della vita privata, acquista particolare importanza.
La circostanza che la Corte di Giustizia abbia ricondotto l'art. 8 CDFUE nell'alveo dell'art. 8 CEDU fa sì che eventuali ingerenze nel diritto alla tutela dei propri dati personali dovranno essere caratterizzate dal perseguimento di uno scopo legittimo ed essere proporzionate, ossia opportune, idonee e necessarie al suo raggiungimento.
Tuttavia, la circostanza che gli articoli 7 e 8 CDFUE, in quanto filiazione dell'art. 8 CEDU, siano tra loro intimamente connessi tanto da integrare un diritto alla vita privata con riguardo al trattamento dei dati personali, non deve tradursi in una mancata valorizzazione delle differenze ontologiche sussistenti tra essi[134].
La distinzione in due distinte disposizioni normative - diritto alla vita privata e diritto alla tutela dei dati personali -, si fa particolarmente apprezzare nell'ambito degli obblighi di *data retention*.
Come correttamente messo in luce dall'avvocato generale, Pedro Cruz Villalòn, il legame tra le due norme dipende dal tipo di dati personali che vengono in considerazione: esistono invero, dati personali in quanto tali, (ad esempio, le generalità) e dati più che personali (come quelli che si riferiscono alla riservatezza della vita privata)[135].

---

[133] Corte di Giustizia dell'Unione Europea, 24 novembre 2011 (C-70/10). La Corte ha, infatti, affermato che l'ingiunzione diretta, da parte di un giudice ad un *service provider*, di adottare sistemi di filtro per impedire agli utenti di utilizzare sistemi di *file sharing*, in violazione delle norme in materia di diritto d'autore, comprime in modo sproporzionato i diritti e le libertà tutelati dagli artt. 8 e 10 della CDFUE e dai corrispondenti artt. 8 e 10 della CEDU. Così, R. FLOR, *Lotta alla "criminalità informatica"*, cit., 126.
[134] Cfr., Corte di Giustizia dell'Unione Europea, 9 novembre 2010, *Volker und Markus Schecke e Eifert,* C-92/09 e C-93/09.
[135] Conclusioni dell'Avvocato Generale, Pedro Cruz Villalòn, presentate il 12 dicembre 2013, nelle cause riunite C-293/12, *Digital RightsIreland Ltd contro The Minister for Communications, Marineand Natural*

Con riferimento ai primi, si pone il problema di garantire all'interessato il controllo sulle modalità del trattamento, comunicazione dello scopo della rilevazione, diritto di accesso, di seguito e di cancellazione: per essi l'art. 8 della Carta costituisce una garanzia adeguata.
Invece, quanto ai secondi, l'esigenza di tutela si estende agli aspetti variegati della vita di una persona che si siano tradotti in dati suscettibili di trattamento informatico.
In questo caso, però, il rischio è che attraverso la loro raccolta si ricostruiscano profili della personalità: d'altronde, sapere con chi una persona comunichi, dove si trovava in un determinato momento, quali siti *Internet* ha visitato negli ultimi due anni, costituisce senza dubbio un'ingerenza nel suo diritto alla riservatezza della vita privata.
Pur considerando che tali dati verranno acquisiti solo se necessari per la repressione di reati gravi, resta il fatto che essi vengono conservati per un apprezzabile lasso di tempo, ingenerando nei cittadini una sensazione di permanente controllo.
Illuminati sono, all'uopo, i principi portati in dote dalla Corte di Strasburgo secondo i quali l'obbligo di conservazione di dati relativi alla vita privata di una persona e alle sue comunicazioni costituisce, di per sé, un'ingerenza nel diritto al rispetto della vita privata e della vita familiare di cui all'art. 7 della Carta di Nizza.
Questo – si badi bene – a prescindere dal fatto che le informazioni memorizzate abbiano carattere sensibile o meno e a prescindere dagli effetti di tale conservazione. Rileva, pertanto, la necessità di verificare se le deroghe rispettino il nucleo essenziale dei diritti in questione; nonché, se siano rispondenti a finalità di interesse generale riconosciute dall'Unione ovvero, infine, se derivino dalla necessità di proteggere diritti e libertà altrui, conformemente al disposto di cui all'art. 52 della Carta.
Ebbene, a parere dei giudici europei, quanto al primo aspetto non si può affermare che la *data retention* pregiudichi il contenuto essenziale dell'art. 7 della Carta di Nizza giacché è escluso che i *provider* e l'autorità giudiziaria vengano a conoscenza del contenuto delle conversazioni.
Non è, parimenti, leso il contenuto essenziale del diritto al trattamento dei dati personali (art. 8 Carta di Nizza), poiché l'art. 7 della Direttiva 2004/26/CE prevede regole specifiche in tema di protezione e sicurezza dei dati.

Resources e altri e C-594/12, *KärntnerLandesregierung Michael SeitlingereChristofTschohl*, in *www.curia.europa.eu.*

Invece, con riguardo al secondo aspetto l'obiettivo della disciplina oggetto dello scrutinio di compatibilità con la Carta di Nizza è individuato nella necessità di garantire la disponibilità dei dati a fini di indagine, accertamento e perseguimento di reati gravi; il che si inserisce nel più generale obiettivo di interesse generale di mantenimento della sicurezza e della pace.
Nonostante ciò, la normativa europea sulla conservazione dei dati di navigazione incontra, secondo la Corte, un insormontabile ostacolo nel principio di proporzionalità, inteso, sulla scia della costante giurisprudenza della stessa Corte, quale capacità di realizzare gli obiettivi perseguiti dalla normativa e senza superare i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi, secondo un giudizio di adeguatezza del mezzo adoperato rispetto al fine[136].
Ed invero, il diritto al rispetto della vita privata rappresenta un diritto fondamentale le cui restrizioni devono palesarsi come strettamente necessarie: ciò, soprattutto, in tutti quei casi in cui la conservazione di dati sensibili avviene automaticamente e laddove vi sia un concreto rischio di *un law ful access and use* di tali dati.
Questi i rilievi critici dei giudici comunitari. In primo luogo, la Direttiva 2006/24/CE concerne ogni comunicazione elettronica o traffico di dati senza alcuna differenziazione a seconda della gravità del reato che si intende accertare; la conservazione riguarda tutti i cittadini dell'Unione, a prescindere da qualsiasi elemento che indichi la commissione di un crimine e da eventuali obblighi di segretezza; inoltre, non vi è alcun rapporto tra il dato immagazzinato e la potenziale minaccia alla pubblica sicurezza[137]
Inoltre, la Direttiva non prevede alcun *objective criteri on* cui ancorare i limiti dell'accesso e conseguente uso dei dati conservati: tra l'altro, non si prevede alcuna specifica procedura per l'accesso al dato, così come non si specifica a quali fini il dato deve essere utilizzato.
Infine, si sottolinea la mancanza di una distinzione a seconda della gravità del crimine nella determinazione della forbice edittale, unitamente all'assenza di un criterio oggettivo in base al quale limitare la conservazione al periodo strettamente necessario.

---

[136] V., per tutti, Case C-343/09, *AftonChemical*, EU:C:2010:419.
[137] In particolare, la conservazione dei dati «isnotrestricted to a retention in relation (i) to data pertaining to a particular time period and/or a particulargeographical zone and/or to a circle of particularpersonslikely to be involved, in one way or another, in a serious crime, or (ii) to personswhocould, for otherreasons, contribute, by the retention of their data, to the prevention, detection or prosecution of seriousoffences». Sono considerazioni che, all'evidenza, ben si adattano anche alla normativa dettata in Italia dal D. lgs 196/2003.

Logico corollario che ne deriva è che, *by adopting Directive 2006/24, the EU legislaturehasexceeded the limitsimposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter*»[341]; di qui l'*exitus* dellaDirettiva.
La conseguenza naturale del *dictum* di illegititmità è destinata a ripercuotersi, sia pure in via soltanto riflessa[342], sulle normative di attuazione degli Stati membri dell'Unione e, dunque, anche della disciplina dettata nell'ordinamento italiano dal Codice *privacy*; anche se dovranno essere le Corti interne a stabilire, caso per caso, la compatibilità delle singole norme di recepimento della Direttiva 2006/24/CE.
Tuttavia, bisogna considerare che i principi dettati dalla Corte Europea appaiono di grande rilevanza, soprattutto, se mutuati sul terreno delle investigazioni informatiche.
Quanto rilevato dai giudici europei, infatti, affievolisce, fino a renderla innocua, quella tesi che individua, nelle investigazioni in ambito digitale, il fine (l'indagine su fatti criminosi, anche gravissimi) che giustifica i mezzi (la reiterata violazione o compressione di diritti e garanzie individuali).
Quanto il *dictum* esso, nell'economia del ragionamento, dovrà rappresentare il punto di partenza per il doveroso ripensamento, in ambito europeo, della normativa in tema di conservazione di dati, nonché per l'interpretazione delle norme vigenti nei singoli ordinamenti in tema di indagini informatiche.

7. *Un nuovo strumento investigativo dall'enorme potenzialità invasiva: il captatore informatico.* Quando si ragiona in ordine al rapporto intercorrente tra scienza, progresso tecnologico e processo l'accostamento più ovvio è quello immediato con la prova scientifica.
Un riflesso istintivo e rivelatore: la scienza come grande facilitatrice e condizionatrice dell'esito processuale.
Questa illusione si è sviluppata nel corso del tempo, sulla scia della famosa sentenza della Corte Federale americana Daubert vs Dow Chemical del 1993[138].
Da allora le prove scientifiche, prima centellinate e tipicizzate in poche e determinate espressioni (dattiloscopica, merceologica, grafologica) hanno addirittura dilagato: alcune si sono rivelate decisive e, persino, rivoluzionarie (come la ricerca e la valorizzazione del *dna*) fino ad assumere un ruolo di indiscussa preminenza nel processo.

[138] Sentenza 28 giugno 1993, Daubert e altri c. Merrell Dow Pharmaceuticals, Inc, in S. LORUSSO, *La prova scientifica*, cit., 310.

La vicenda legata all'omicidio di Yara Gambirasio, probabilmente, segna un punto di non ritorno: la rilevazione genetica oscura ogni altro elemento indiziante: non esiste neanche la prova che l'imputato avesse mai conosciuto o addirittura visto la sua vittima, ma una macchia sugli indumenti ha assorbito ogni considerazione, argomentazione e/o confutazione dialettica.
La voce della scienza tacita tutte le altre.
Ma non è finita: una nuova avanzatissima, quanto invasiva, tecnologia appare sul proscenio nella espressione estrema del "*captatore informatico*" – meglio sarebbe chiamarlo con nome proprio di virus informatico –, strumento dotato di un'efficacia devastante[139].
Il *software* maligno si insinua nei *computers* e nei *devices* mobili di ultima generazione e parassitariamente penetra nei più remoti recessi dell'apparecchio, "*succhia*" corrispondenza, messaggi ed addirittura come se non bastasse, funziona da microfono e telecamera a cielo aperto in tutti gli ambienti in cui l'intercettato si muove, senza la barriera di alcuna intimità[140].

---

[139] Su questo nuovo strumento, cfr., E. APRILE, *voce Captazioni atipiche (voci, immagini, segnali),* in A. SCALFATI (diretto da), *Dig. disc. pen.,* Torino, 2012, 1; S. ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del* cloud criminal, in G. COSTABILE, A. ATTANASIO, (a cura di), *IISFA Memberbook 2012 Digital Forensics. Condivisione della conoscenza tra i membri dell'IISFA ItalianChapter*, Sassari, 2013, 1 ss.; S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *questa rivista*, 2014, 2; S. MARCOLINI, *Le cosiddette perquisizioni on line (perquisizioni elettroniche)*, in *Cass. pen.*, 2010, 2855 ss.; Id, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015, 760; M. TROGU, *Sorveglianza e "perquisizioni" online su materiale informatico,* in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, 431. Per un'analisi comparata con specifico riferimento all'esperienza tedesca, cfr. R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung,* cit., 679 ss.; quanto all'esperienza statunitense, v. F. CERQUA, *Le investigazioni informatiche e la protezione dei dati personali negli Stati Uniti e in Italia: due modelli a confronto*, in P. CORSO, E. ZANETTI, (a cura di), *Studi in onore di Mario Pisani, II, Diritto processuale penale e profili internazionali: diritto straniero e diritto comparato,* Piacenza. 2010, 775.

[140] Publio Virgilio Marone nel libro II dell'Eneide, 49, narra "*TimeoDanaos et dona ferentes...*" ma i Troiani non dettero ascolto al grido di allarme di Lacoonte e portarono il cavallo all'interno delle mura, convinti dei buoni propositi dei greci e che quel dono fosse il segno tangibile della fine delle ostilità. E così, è noto a tutti, il destino della città di Ilio trovò il suo tragico epilogo. L'astuto Ulisse aveva ideato e portato a compimento il piano che, poi nei secoli, è diventato la metafora entrata nel linguaggio comune per definire qualsiasi stratagemma atto a penetrare le difese, il paradigma per antonomasia dell'intrusione occulta che porta ad ottenere il risultato avuto di mira. Non a caso, è proprio nella vicenda del Cavallo di Troia che troviamo l'etimologia della parola "*Trojanhorse*", termine con il quale nella sicurezza informatica si definisce un software c.d*malware*(cioè dannoso), che ha la caratteristica di nascondere il suo funzionamento all'interno di un altro programma apparentemente utile o innocuo, oppure che è inserito in allegato ad una e-mail, ed è inviato alla sua destinazione "da re-moto"; nel momento in cui esegue la finta applicazione o il presunto aggiornamento o legge il messaggio di posta elettronica, l'utente attiva anche il *virus*, che – come i guerrieri achei guidati da Ulisse – si autoinstalla nell'apparecchio o nel sistema e lo conquista, comunicando il contenuto (a seconda del caso, di vario ge-nere) a un recettore. Il *malware* attacca indifferentemente *tablet*, *pc*, *smartphone* ed agisce, a differenza del dilagare dei guerrieri greci

Tempo verrà che il "*virus*" (perchè tale è) potrà propalarsi da un terminale all'altro contagiando epidemicamente anche coloro che venissero in contatto col portatore.
La funerea previsione di Orwell è ad un passo[141].
Sembra lontanissimo il 2002, anno in cui le Sezioni Unite, con la famosa sentenza Franzese[142], fissarono le tavole dell'argomentazione scientifico-giuridica tracciandone il confine in modo netto: la scienza è un mezzo come un altro, interfungibile pure con le "*massime di comune esperienza*" e comunque gerarchicamente sottoposto alla eccellenza dialettica della confutazione controfattuale.
L'assunto si fondava sul fatto che anche il calcolo probabilistico più accurato non poteva sostituire il ragionamento induttivo – indiziario: la macchina finisce là dove inizia la mente umana.
Oggi le cose sono mutate radicalmente e l'impressione è che ci si trovi in un mondo nuovo con a capo la "*prova totalitaria*". Le tecniche assorbono nella loro avanzata ed invasiva perfezione ogni possibile contraria confutazione.

---

dentro le mura di Troia, in modo del tutto occulto, ma con la stessa capacità che ebbero le armi degli achei. Fuori dalla metafora, se queste sono le caratteristiche dei *virus trojan*, non stupisce per niente che un simile strumento sia stato ritenuto utile a livello investigativo, viste le informazioni (elementi di prova) che, tramite il suo utilizzo, è teoricamente possibile apprendere al fascicolo delle indagini: conversazioni, fotografie, video, messaggi di posta elettronica, dati contenuti nell'*hard disk*, persino in presa diretta nel momento in cui il soggetto digita lettere e numeri sulla tastiera dello strumento sottoposto alla captazione.

[141] G. ORWELL, *1984*, Milano, 2002, 3 ss., naturalmente non era possibile sapere se e quando si era sotto osservazione. Con quale frequenza o con quali sistemi, la Psicopolizia si inserisse sui cavi dei singoli era oggetto di congettura. Si poteva persino presumere che osservasse tutti continuamente. Comunque fosse, si poteva collegare al vostro apparecchio quando voleva. Dovevate vivere (e di fatto vivevate, in virtù di quella abitudine che diventa istinto) presupponendo che qualsiasi rumore da voi prodotto venisse ascoltato e qualsiasi movimento - che non fosse fatto al buio – attentamente scrutato.

[142] La letteratura in argomento è ampia v., per tutti, R. BARTOLI, *Causalità omissiva e modello di accertamento ex ante – post*, in *Cass. pen.*, 2006, 3219; G. BILLO, *L'indagine causale nell'ambito del settore medico alla luce delle indicazioni delle Sezioni Unite: profili problematici e spunti applicativi*, in *Ind. pen.*, 2008, 339; R. BLAIOTTA, *"La causalità nella responsabilità professionale. Tra teoria e prassi"*, Milano, 2004, 34 ss.; C. BRUSCO, *La causalità giuridica nella più recente giurisprudenza della Corte di Cassazione*, in *Cass. pen.*, 2004, 2599; F. CAPRIOLI *La scienza cattiva maestra: le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, 3520; G. CANZIO, *"La causalità scientifica"*, in *Dir. proc. pen.*, 2008, *Dossier*, 38; G. F. IADECOLA, *La causalità dell'omissione nella responsabilità medica prima e dopo le Sezioni Unite Franzese*, in *Riv. it. dir. proc. pen.*, 2005, 609; L. MASERA, *Il modello causale delle Sezioni Unite e la causalità omissiva*, in *Dir. pen. proc.*, 2006, 493; A. PAGLIARO, *Causalità e diritto penale*, in *Cass. pen.*, 2005, 1037; F. STELLA, *Etica e razionalità del processo penale nella recente sentenza sulla causalità delle Sezioni Unite della Suprema Corte di Cassazione. Nota a Cass. Pen., S.U., ud. 10.7.2002, dep. 11.9.2002, n. 30328, Franzese*, in *Riv. it. dir. proc. pen.*, 2002, 767; Id., *Verità, scienza e giustizia: le frequenze medio – basse nella successione di eventi. Nota a Cass. Pen., S.U., ud. 10.7.2002, dep. 11.9.2002, n. 30328, Franzese,* in *Riv. it. dir. proc. pen.*, 2002, 1215.

Cosa si può obiettare? Quale spazio resta alla ragione umana per controbattere? E del resto già si aggiunge la prossima utopia finale: la riproduzione delle sinapsi umane in una macchina.
L'epistemologo Charles Percy Snow, appena pochi decenni fa, parlava ancora di "*due culture*" e sognava di arrivare ad un unico canone che le fondesse[143].
Oggi il timore è che la regola scientifica spazzi via l'ermeneutica ed ogni necessità di rifarsi alla logica umana. Timore fondato posto che la valutazione giurisdizionale e probatoria non è mai un fatto automatico o scientifico ma è il frutto di un ragionamento che tiene insieme gli elementi legittimamente.
Peraltro, gli strumenti di cui stiamo parlando hanno, in sé, la caratteristica intrinseca di essere capaci di scrutare e "spiare" interamente e perpetuamente l'individuo.
Non resta, allora, che chiedersi: quali sono i limiti entro cui è consentito allo Stato di controllare la vita dei cittadini?.
In questo caso, il progresso scientifico (ma non solo) mette a disposizione degli operatori strumenti sempre più efficaci che consentono un penetrante controllo mirato (intercettazioni, telefoniche ed ambientali, di flussi di dati, localizzazioni con *gps*, ecc.) ed un costante tracciamento di dati (movimenti bancari, telepass, riprese video a circuito chiuso, dati di navigazione internet) cui si può attingere per ogni esigenza investigativa.
Tale capacità deve, però, confrontarsi con le prerogative e i diritti di ogni individuo che indicano un principio di fondo: le libertà costituzionalmente e convenzionalmente garantite possono essere conculcate e limitate solo in condizioni eccezionali e per ragioni precise ed in ogni caso nei limiti previsti dalla legge costituzionalmente valida.
E', forse, il caso di cominciare a prendere atto che non tutto quello che è tecnologicamente possibile acquisire risulta anche compatibile con i principi garantiti a livello nazionale e sovranazionale.
In fondo è questo il senso del limite che, a volte, sembra mancare.
Tra l'altro, occorre tener conto che spesso la legge è costretta ad inseguire un'evoluzione scientifica che si presenta sempre più rapida ed imprevedibile e, nel lasso temporale intercorrente tra il nuovo strumento investigativo e

[143] CHARLES PERCY SNOW, *Le due culture*, Marsillo, 2005, p. 3 ss., Snow, che era al tempo stesso fisico e scrittore, in questo libro descrive una vera e propria spaccatura tra il mondo della ricerca scientifica e quello degli studi umanistici. Questo problema di comunicazione e di scambio di esperienze si traduce quasi in una spartizione di raggi d'azione: mentre la ricerca scientifica e tecnologica detiene una grande importanza nello sviluppo sociale di una comunità, la cultura umanistica domina le scelte di carattere politico. Secondo Snow, in entrambi gli ambiti, sociale e politico, sarebbe invece necessaria la presenza delle due culture che, pur creando punti di vista divergenti, si arricchirebbero reciprocamente, assicurando una certa profondità di prospettiva.

l'intervento del legislatore, la tutela dei diritti del cittadino è affidata alla prassi giurisprudenziale che è orientata a tutelare esigenze, vere o presunte, di sicurezza sociale e non i diritti dell'indagato.
E' importante, dunque, saper cogliere tali aspetti cristallizzandoli in una legge che tenga conto di queste esigenze, soprattutto in considerazione del recente intervento nomofilattico operato dalle Sezioni Unite le quali hanno, di fatto, selezionato gli ambiti di operatività del captatore informatico mettendo in luce, però, diverse criticità[144].
Nelle attuali tipologie configurative, tale strumento è in grado di aprire le impostazioni di sistema, di attivare l'impianto microfonico del *device* (e fare quindi da registratore vocale), di comandare in modo silente lo *start* della telecamera (e quindi funzionare da apparato clandestino di video ripresa), di generare uno *screen shot* dello schermo, di gestire la localizzazione *gps*, di effettuare operazioni di *sniffing* tra le cartelle di posta, delle foto, di scartabellare tra i *folder* dei documenti, nelle applicazioni di messaggistica *end to end*, sui profili *social*, o di una video *chat* crittografata[145].
Insomma, un insidioso applicativo silenzioso, in grado di catturare tutti quei dati che, nel corso di una tradizionale intercettazione telematica, non possono essere forzati in apertura dall'operatore, seppur presenti nella griglia *excel* di storico dei dati, per via di quel "*lucchetto*" che protegge il sistema con il protocollo HTTPS.
Si tratta, cioè, di un espediente che, allo stato dell'arte, non è solo idoneo all'effettuazione di una intercettazione giudiziaria di conversazioni, di comunicazioni telefoniche, di altre forme di telecomunicazione o di una intercettazione di comunicazioni tra presenti (art. 266 commi 1 e 2 c.p.p.), o ancora di mera intercettazione di comunicazioni informatiche o telematiche (art. 266 *bis* c.p.p.), bensì di un captatore che ha le potenzialità di perquisire, sequestrare, cancellare i contenuti di un apparato elettronico, da qui violando *privacy*, riservatezza, domicilio virtuale di un bersaglio investigato, ma anche alterare, inquinare o distruggere la *crime scene* informatica.

8. ***Il punto delle Sezioni unite: dubbi irrisolti?.*** Le Sezioni unite dalla Corte di cassazione, consapevoli delle capacità intrusive e delle potenzialità cognitive del *software* maligno sono intervenute per cercare di risolvere la *vexata questio* relativa ai presupposti e alla possibilità di utilizzare questo strumento al-

[144] Il riferimento è a Cass. sez. un., 28 aprile 2016, n. 26889, con nata a cura di P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforme*, in *Proc. pen. gius.*, 2016, 118 ss.
[145] L'argomento è stato approfondito da M. TORRE, *Il captatore informatico*, cit., 32 ss.

tamente invasivo durante le indagini: l'intervento si è risolto attraverso l'esegesi del dato normativo in materia di intercettazioni di comunicazioni e di conversazioni tra presenti, con specifico riferimento sia alla disciplina codicistica, sia a quella speciale in tema di reati di criminalità organizzata (art. 13 d.l. n. 152/1991).

La sentenza si inserisce in un particolare contesto caratterizzato da un vuoto normativo ed ha costituito un importante monito per il legislatore, chiamato a disciplinare la materia facendosi carico dei problemi, vecchi e nuovi, che connotano questa peculiare *species* di prova scientifica[146].

Ancora una volta alla Corte si è imposto, *in primis*, di risolvere il delicato problema di bilanciare le esigenze investigative con i diritti fondamentali dell'individuo oggetto di possibili lesioni[147].

Pur mancando, in questa materia, una specifica regolamentazione ciò non vuol dire che le attività investigative debbano ritenersi vietate e, come tali, non idonee a fornire elementi probatori utili allo sviluppo delle indagini e alla decisione del giudice.

Infatti, alcune di tali attività sono riconducibili alla categoria dei mezzi di ricerca della prova, di già regolati da specifiche norme di legge (ad esempio le intercettazioni), altre, invece, trovano legittimazione nel processo grazie al principio generale di non tassatività della prova in virtù del quale il giudice è autorizzato ad assumere anche prove non vietate dalla legge purchè siano idonee all'accertamento dei fatti e non pregiudichino la libertà morale della persona interessata (art. 189 c.p.p.)[148].

L'art. 189 c.p.p., dunque, si caratterizza per essere una disposizione a due volti: ammette e respinge, accoglie ed esclude: da un lato, una norma di apertura che consente l'ingresso nel processo di strumenti conoscitivi non regolati, dall'altro, una norma di chiusura che sbarra la strada ad ogni procedimento probatorio vietato.

Nel caso del *softwar*e maligno è fuor di dubbio che si tratti di uno strumento idoneo (ed utile) all'accertamento dei fatti che non pregiudica la libertà morale dell'indagato[149].

---

[146] P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforme*, cit. 1.

[147] Cass. sez. un., 28 aprile 2016, n. 26889, in *Mass. Uff.* n. 260965.

[148] In tema F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova, in Italia*, in *RavBras de Diretto Processual – penal*, Porto Alegre, 2017, 493.

[149] Cass. Sez. IV, 16 marzo 2000, n. 7063, in *Dir. pen. proc.*, 2001, 81. In dottrina, v., F. CAPRIOLI, *Riprese visive nel domicilio e intercettazioni "per immagini"*, in *Gius. cost.*, 2003, 2187.

Pertanto, in linea di principio, l'utilizzo di tale strumento può essere ammesso anche se non specificamente previsto dalla legge.
Tuttavia, anche se si tratta di prove atipiche ne è, comunque, vietato l'utilizzo laddove queste incidano, conculcandoli, sui diritti tutelati dagli artt. 13, 14, e 15 Cost., a meno che non siano assunte in attuazione di un provvedimento motivato emesso dall'Autorità giudiziaria nei casi previsti dalla legge[150].
In altre parole, occorre che sia la legge ordinaria a disciplinare in quali casi, con quali modalità e con quali garanzie i diritti costituzionali possono essere violati: ciò, in armonia con quanto previsto dall'art. 8 CEDU[151].
Una parte della critica ha ritenuto che il *softwere* maligno, poiché strumento capace di conculcare il bene giuridico protetto dalla doppia riserva – legge/giurisdizione – rientra, a pieno titolo, nella categoria delle prove incostituzionali[152], considerata la fisiologica inidoneità dell'art. 189 c.p.p. ad adempiere alle riserve previste dall'art. 14 Cost.: conseguentemente, gli esiti probatori saranno soggetti alla sanzione dell'inutilizzabilità in virtù del divieto implicito sotteso all'art. 189 c.p.p.[153]
La voce unanime dell'interprete è, però, rivolta a richiedere l'attenzione sulla necessità che la prova atipica che, per definizione non è volta a destrutturare i modelli tipici previsti dal codice di rito, quanto piuttosto ad integrare il sistema probatorio, non venga strumentalizzata per aggirare i requisiti delle prove tipiche: dal codice, invero, si ricava un principio di non sostituibilità in forza del quale è vietato l'aggiramento delle forme probatorie poste a garanzia dell'imputato o dell'attendibilità dell'accertamento: in tal senso si configura un vero e proprio divieto probatorio a pena di inutilizzabilità degli elementi acquisiti[154].
Ma allora come si colloca il *virus* all'interno del codice? Cioè qual è la sua esatta qualificazione giuridica?.

---

[150] Cfr., F. IOVINE, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenzedi accertamento penale*, in *Riv. trim. dir. pen. cont.*, 2014, 336.
[151] In argomento, cfr., S. ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del cloud criminal*, in G. COSTABILE, A. ATTANASIO (a cura di), Sassari, 2013, 1; S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *questa rivista*, 2014, 194.
[152] M. TORRE, *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. proc.*, 2015, 1168; Per la inconvenzionalità della prova atipica, E. ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tuteladella privacy e onde eversive*, in *questa rivista*, 2015, 9; L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante: le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, in *questa rivista*, 2016, 349; *contra*, M. DANIELE, *Indagini informatiche lesive della riservatezza. Verso una inutilizzabilità convenzionale?*, in *Cass. pen.*, 2013, 367.
[153] Cfr., P. TONINI, C. CONTI, *Il diritto delle prove penali*, cit., p. 392.
[154] P. TONINI, C. CONTI, *Il diritto delle prove penali*, cit., 200.

Ebbene, esso non può essere inquadrato nello schema della perquisizione ordinaria (artt. 247-242 c.p.p.) ne, tantomeno, in quello inerente la perquisizione c.d. informatica (art. 247 comma 1 *bis* c.p.p.) poiché, a differenza di questi atti che sono regolati dalla legge, esso si sostanzia in un'attività permanente, occulta ed ignara alla persona che dispone dell'oggetto da perquisire, volta all'acquisizione indiscriminata di dati senza possibilità di selezionare solo quelli che effettivamente si riferiscono al fatto da accertare[155].
La giurisprudenza, pur cogliendo tali aspetti si mostra, invece, favorevole ad ammettere l'acquisizione di dati a carattere non comunicativo da parte del captatore[156].
Opzione interpretativa quest'ultima non condivisa dalla dottrina la quale, viceversa, valorizzando un concetto più ampio di domicilio, ha rilevato che la tutela sottesa all'art. 14 Cost. si estende anche al domicilio informatico, cioè a quello spazio virtuale che ciascun individuo occupa nell'universo digitale[157].
Tra l'altro, esiste una protezione informatica dell'individuo destinata ad ampliare i confini del diritto all'intimità della vita privata e al rispetto della dignità personale[158]: un nuovo ed ulteriore spazio virtuale al cui interno – esattamente come nel domicilio e nei circuiti comunicativi riservati – ciascuno deve essere in grado di sviluppare liberamente la propria personalità al riparo dei "*virus spie*"[159].
In questa prospettiva la Corte costituzionale tedesca nel 2008 ha affermato l'esistenza di un apposito diritto fondamentale – "*il diritto all'uso riservato e confidenziale delle tecnologie informatiche*" – derivato dalla dignità della persona, matrice dei diritti fondamentali[160].

---

[155] A. TESTAGUZZA, *I sistemi di controllo remoto: fra normativa e prassi*, in *Dir. pen. proc.*, 2014, 759; M. TROGU, *Sorveglianza e "perquisizioni" online su materiale informatico*, cit., 444. In giurisprudenza, Cass., Sez. IV, 17 aprile 2012, n. 19618, in *Cass. pen.* 2013, 1523

[156] Cass., Sez. V, 14 ottobre 2009, n. 16556, in *Mass. Uff.* n. 246954.

[157] In questi termini, v., F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova*, cit., 498.

[158] F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen.*, 1967, 1120.

[159] In tema, L.GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Riv. trim. dir. pen. cont.*, 2017, 1.

[160] Si tratta della sentenza del *Bundesverfassungsgericht* 27 febbraio 2008, in *RTDPE*, 2009, p. 609, con nota di R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung* con la quale è stata riconosciuta l'inadeguatezza dei diritti a tutela delle libertà didomicilio e delle comunicazioni a dare copertura sufficiente allo spazio digitale, ed è stato inaugurato un nuovo diritto costituzionale riconducibile alla c.d. "autodeterminazione informativa" e "sicurezza informatica", quest'ultima da intendersi anche come integrità e riservatezza dei dati e delle informazioni trattate da sistemi informatici, fondato sulla dignità umana dell'individuo e dell'utente "informatico". Nel 2016 è intervenuta un'altra pronuncia (Bundersverfassungsgericht, I Senato, 20 aprile 2016, 1 BVR 966/09, 1 BVR

Ed è proprio questo il versante che dovrebbe essere preso come riferimento dal nostro ordinamento giuridico: la Corte costituzionale, in particolare, dovrebbe estrapolare dall'art. 2 Cost (clausola aperta) il nuovo diritto fondamentale alla riservatezza informatica[161].
Ragionando in questi termini, però, rimarrebbe da definire l'esatto perimetro della tutela sovranazionale posto che il diritto sarebbe privo della doppia riserva[162].
Le Sezioni Unite hanno tentato di risolvere (definitivamente) il problema facendo ricorso alla disciplina prevista per le intercettazioni ambientali[163] rilevando che dall'esegesi dell'art. 266 c.p.p. si evince che la norma autorizza, negli stessi casi previsti dal primo comma, l'intercettazione delle comunicazioni tra presenti: ove il riferimento all'ambiente è presente solo nella seconda parte della disposizione in relazione, però, alla tutela del domicilio[164].
La Corte si è posta il problema della valenza da attribuire all'individuazione del luogo in cui si deve svolgere l'intercettazione trattandosi di bene coperto dalla tutela costituzionale e sovranazionale: in sostanza, si è messa in evidenza l'alternativa interpretativa in ordine alla configurabilità o meno

---

1140/09, in *Riv. trim, dir. pen. con.*, 2016, 12, con nota di 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*, con la quale è stato ribadito che, anche nel caso di investigazioni compiute per mezzo di strumenti tecnologici che garantiscono l'accesso da remoto ai sistemi informatici, va garantito il nucleo della vita privata ("*Kernbereichprivater Lebensgestaltung*" nella versione originale tedesca, "*core area of private life*", nella traduzione inglese del comunicato stampa della Corte), non tutelato adeguatamente, secondo la Corte, dal paragrafo 20k della legge federale denominata "*Bundeskriminalamtgesetz*" – *BKAG* – che disciplina i compiti e l'attività della forza di polizia federale, la quale prevede il controllo dei dati raccolti ad opera del personale dell'ufficio federale di polizia penale e non di soggetti esterni e indipendenti. Al riguardo, infatti, va segnalato che la disciplina delle intercettazioni in Germania è caratterizzata dall'intangibilità assoluta del nucleo caratterizzante la vita privata e dal controllo politico-parlamentare. Cfr. F. RUGGIERI, *Le intercettazioni e la sorveglianza di comunicazioni e dati nei Paesi di area tedesca*, in *Le intercettazioni di conversazioni, Un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti, Atti del Convegno dell'Associazione tra gli studiosi della procedura penale*, Milano, 2007, 218.

[161] R. ORLANDI, *Osservazioni sul documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici*, in *Aech. pen.*, 2016, 32.

[162] In questi termini F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova*, cit., 499.

[163] La corte si è discostata dal precedente orientamento maggioritario secondo cui le videoriprese effettuate da remoto, mediante l'attivazione attraverso il c.d. virus informatico della telecamera di un apparecchio telefonico smartphone, possono ritenersi legittime quali prove atipiche ai sensi dell'art. 189 cod. proc. pen., salvo che siano effettuate all'interno di luoghi di privata dimora, e ferma la necessità di autorizzazione motivata dall'A.G. per le riprese che, pur non comportando una intrusione domiciliare, violino la riservatezza personale. Cfr., Cass. Sez. VI, 25 maggio 2015, n. 27100, in *Mass. Uff.* n. 265665.

[164] Si veda M. T. ABBAGNALE, *In tema di captatore informatico*, in *questa rivista*, 2016, 459.

dell'indicazione (e della predeterminazione) del luogo come requisito indispensabile di legittimità della ricerca probatoria.
Sulla base di questo è stato ritenuto che non occorre che nel provvedimento autorizzativo venga indicato il luogo perché le caratteristiche tecniche dell'intercettazione mediante *virus* informatico prescindono da tale riferimento trattandosi di un'intercettazione ambientale "*itinerante*"[165].
Da ciò deriva che la specificazione del luogo ove effettuare l'intercettazione mediante *virus* informatico non è elemento necessario[166] per cui un'eventuale inosservanza non inficia il provvedimento autorizzativo e che deve essere esclusa la possibilità di espletare intercettazioni nei soli luoghi indicati dall'art. 614 c.p. al di fuori della disciplina derogatoria di cui all'art. 13 d.l. n. 152/1991[167]: ciò in quanto nelle intercettazioni regolate dall'art. 266 e ss. c.p.p. il requisito sotteso al provvedimento autorizzativo incentrato sul fondato motivo di ritenere che nei luoghi di cui all'art. 614 c.p. si stia svolgendo l'attività criminosa, si pone in tutta la sua pienezza non consentendo eccezioni di alcun tipo[168].
Solo quando si tratta di luoghi di privata dimora il decreto autorizzativo delle intercettazioni tra presenti deve contenere la specifica indicazione dell'ambiente nel quale la captazione deve avvenire: invece, nei casi in cui questa si dovrà svolgere nei luoghi diversi da quelli indicati dall'art. 614 c.p., sarà sufficiente che il decreto indichi il destinatario e la tipologia di ambienti dove dovrà essere eseguita[169].
Il ragionamento, però, non ha convinto. Infatti, anche se il *virus* informatico è stato considerato "*itinerante*", prima o poi, si corre il rischio che finisca per registrare colloqui all'interno di un domicilio: in questo caso, è stato ipotizza-

---

[165] Ampiamente A. GAITO, S. FURFARO, *Le nuove intercettazioni "ambientali" tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *questa rivista*, 2016, 316.
[166] Tra l'altro, le Sezioni Unite rilevano che nemmeno nella giurisprudenza della Corte Edu si possono trovare riscontri alla necessità di predeterminare l'ambiente di svolgimento delle operazioni di captazione. In effetti, nemmeno l'art. 8 CEDU impone di indicare in via preventiva alcun luogo. Gli elementi richiesti per la compatibilità della disciplina interna sulle intercettazioni con la Convenzione EDU sono stati chiaramente identificati nella sentenza della Corte di Strasburgo *Zackharov c. Russia* del 4 dicembre 2015, in tre parametri fondamentali: base giuridica appropriata, finalità legittima e necessità all'interno di una società democratica. Di recente Cfr. Corte EDU, *Capriotti c. Italia*, 23 febbraio 2016, che fornisce legittimità a quella prassi di intercettazioni telefoniche compiuta su suolo italiano ma relativa a comunicazioni effettuate all'estero, mediante il c.d. *instradamento*.
[167] Al riguardo, G. LASAGNI, *L'uso di captatori informatici (trojan) nelle intercettazioni "fra presenti"*, in *Riv. trim. dir. pen. cont.,* 2016, 15.
[168] Per un quadro più ampio, cfr., F. CAJANI, *Odissea del captatore informatico*, in *Cass. pen.,* 2016, 4146.
[169] Costituisce intercettazione la captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti attuata da un estraneo con strumenti tecnici di percezione che vanificano le tutele poste a presidio della riservatezza. Cass. sez. un., 28 maggio 2003, n. 36747, in *Cass. pen.*, 2004, 2094.

to che l'autorizzazione del giudice potrebbe essere circoscritta alle conversazioni che avverranno in un determinato luogo pubblico o aperto al pubblico[170].

Il *virus*, inoltre, potrebbe essere contenuto in un *personal computer* installato in un determinato posto non domiciliare e non trasportabile[171] ovvero collocato in un portatile abitualmente tenuto fermo[172].

Non si dimentichi che esso permette di "*impossessarsi*" dell'*hardwere* e di attivare alcune funzioni – ad esempio, il microfono, la telecamera, il *gps* ecc. – trasformando il dispositivo in uno strumento capace di fotografare, riprendere l'ambiente circostante, registrare le conversazioni in prossimità e di localizzare con precisione altri dispositivi di comunicazione[173]: infine, il captatore consente di prendere il completo controllo del dispositivo e può, senza alcuna difficoltà, cancellare informazioni o inserirne di nuove[174]

Sono questi alcuni degli aspetti che evidenziano i limiti strutturali della decisione delle Sezioni Unite[175]

Tuttavia, proprio queste obiezioni consentono di cogliere la scelta intrapresa dalla Corte la quale non ha voluto legittimare l'adozione di un'autorizzazione di intercettazioni *al buio*, cioè concessa senza poter valutare preventivamente lo svolgimento di attività criminose nel luogo domiciliare in cui potrebbe essere introdotto il dispositivo.

Nella sentenza viene precisato che "*se anche fosse tecnicamente possibile seguire gli spostamenti dell'utilizzatore del dispositivo elettronico e sospendere la captazione nel caso di ingresso in un luogo di privata dimora, sarebbe comunque impedito il controllo del giudice nel momento dell'autorizzazione*": quindi, si è voluto evitare alla radice il rischio di realizzare intercettazioni tra presenti in luoghi di privata dimora[176].

---

[170] Ampiamente, A. CAMON, *Cavalli di troia in Cassazione*; in *Cass. pen.*. 2016, 2274.

[171] L'esempio è tratto da G. AMATO, *Reati di criminalità organizzata: possibile intercettare conversazioni o comunicazioni con un captatore informatico*, in *Guida dir.,* 2016, n. 34, 79.

[172] 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, 161.

[173] In dottrina si vedano i contributi di, E. ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della privacy e onde eversive*, cit., 8; F. DITARANTO, R. RUGGIERI, V, CAPELLI, *Nuove tecniche d'investigazione nell'era digitale: il "malwere" di Stato*, in *Cyb. dir.*, 2017, 113; L. MONTEVERDE, *Le nuove "frontiere" delle intercettazioni*, in *questa rivista*, 2014, 3; A. TESTAGUZZA, *Exitus acta probat. "Trojan" di Stato: la composizione di un conflitto*, in *questa rivista*, 2016, 1 ss.

[174] Cfr. G. ZICCARDI, *Parlamento europeo, captatore informaticoe attività di hacking delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche*, in *questa rivista*, 2017, 1 ss.; Id., *L'odio online*, Milano, 2016, 51 ss.; Id., *Internet, controllo e libertà*, Milano, 2015, 32 ss.; Id., *Hacker, il richiamo della libertà*, Venezia, 2011, 3 ss.

[175] Il profilo è stato approfondito da F. CAJANI, *Odissea del captatore informatico*, cit., 4149.

[176] In questa prospettiva le Sezioni Unite hanno ritenuto insoddisfacente la tutela "*postuma*" delle preroga-

Certo, il legislatore del 1988 non avrebbe potuto immaginare che a "*recuperare*" le informazioni sarebbe stato un oggetto virtuale in possesso della stessa persona intercettata destinato a seguirla in ogni spostamento della sua vita privata al punto da conculcare seriamente la sua *privacy*[177].
Tra l'altro, il fatto che nella disciplina codicistica manchi uno specifico riferimento alla tipologia degli strumenti di captazione, rende ancor più evidente il *vulnus* e più urgente l'intervento riparatore da parte del legislatore: bisogna considerare che nel mondo 2.0 sono presenti modalità diversificate – e assai diversamente aggressive – di attacco alla sfera comunicativa riservata[178].
Una normativa che non prende in considerazione questi aspetti o, per lo meno, si mostra incapace di disciplinarli rispettando i diritti fondamentali, è lacunosa e tecnicamente obsoleta prestandosi a letture evolutive che la rendono intollerabile ai presidi della Carte Fondamentale[179].
Ma, l'intervento nomofilattico va scandagliato anche da un'altra angolazione.
A parere dei Giudici, invero, l'utilizzo del *softwere* maligno è consentito nei casi eccezionali in cui la legge autorizza l'intercettazione domiciliare anche in assenza dello svolgimento attuale di un' attività criminosa e cioè nei casi in cui

---

tive individuali che potrebbe derivare dall'applicazione della sanzione dell'inutilizzabilità che colpirebbe le sole intercettazioni eventualmente avvenute in luoghi di privata dimora al di fuori dei presupposti di cui all'art. 266, comma 2, c.p.p.: l'inutilizzabilità, infatti, va riservata a gravi patologie degli atti del procedimento e non all'ipotesi di adozione di provvedimenti *contra legem* e non preventivamente controllabili quanto alla loro conformità alla legge. Cfr. L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, cit. 7.

[177] Basti pensare, come rileva Cass. sez. un., 28 aprile 2016, n. 36889, cit., che "il soggetto intercettato può recarsi, portando con sé l'apparecchio elettronico nel quale è stato installato il "captatore", nei luoghi di privata dimora di altre persone, così dando luogo ad una pluralità di intercettazioni domiciliari.

[178] In senso contrario si è espressa G. LASAGNI, *L'uso di captatori informatici*, cit., 11, secondo cui il rispetto della doppia riserva di legge e di giurisdizione richiesta dalla Costituzione per ogni tipo di intrusione nelle libertà fondamentali poste a tutela del domicilio privato e delle comunicazioni non si estende – nel quadro normativo vigente – anche alla necessità di avere una specifica previsione legislativa per ogni tipologia di strumento captativo utilizzabile, sul presupposto che la disciplina delle intrusioni tecnologiche nella sfera privata sarebbe tendenzialmente indifferente al tipo di tecnologia utilizzata, come dimostrato anche dai principi ispiratori della nuova normativa europea in materia di protezione dei dati personali (Direttiva UE 2016/280 del Parlamento Europeo e del Consiglio del 27 aprile 2016, *Protezione delle persone fisiche con riguardo altrattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati*). Secondo l'Autrice, sarebbe, quindi, auspicabile un intervento legislativo che identificasse chiaramente non tanto tutte le singole tecnologie utilizzabili nel campo delle intercettazioni (che prima erano microspie, oggi sono *virus* informatici, ma potrebbero ovviamente a breve avere anche forma ben diversa, quanto piuttosto le garanzie fondamentali che devono essere sempre riconosciute all'indagato e aiterzi potenzialmente coinvolti, a prescindere dallo strumento utilizzato.

[179] Per analoghe considerazioni si veda il documento redatto nel luglio 2016 da un gruppo di studiosi di Diritto processuale penale dell'Università di Torino, successivamente sottoscritto da più di settanta docenti universitari di Diritto, in *www.dgunito.it*.

si procede per delitti di criminalità organizzata (art. 13 d.l. n. 152/991): in questa situazione l'indicazione del luogo risulterebbe del tutto irrilevante, poiché in materia di delitti di criminalità organizzata, il legislatore ha operato uno specifico bilanciamento di interessi optando per una più pregnante limitazione della segretezza delle comunicazioni e della tutela del domicilio, tenuto conto dell'eccezionale gravità e pericolosità, per la collettività, dei particolari reati oggetto dell'attività investigativa[180].

In questa situazione, non è necessario indicare la preventiva individuazione dei luoghi e non occorre dimostrare che in essi si stiano svolgendo attività criminose.

Dunque, se da un lato, sembra non destare problemi la duplice prospettiva entro la quale l'organo nomofilattico ha ricostruito la disciplina delle intercettazioni tra presenti, assai meno rassicurante appare la dilatazione del concetto di criminalità organizzata che finisce di svuotare di contenuto il rapporto regola/eccezione, riferibile alla disciplina generale delle intercettazioni (art. 266 comma 2 c.p.p.) e a quella speciale di cui all'art. 13 d.l. n. 152/1991[181].

Le Sezioni Unite hanno optato per una nozione ampia di criminalità organizzata omnicomprensiva non solo dei reati associativi previsti da specifiche norme ma anche di qualsiasi tipo di associazione a delinquere ex art. 416 c.p.[182] correlata alle attività criminose più diverse, compresso il complesso di reati associativi di natura terroristica, con esclusione del mero concorso di persone nel reato[183].

Epperò, anche questo specifico profilo desta qualche perplessità: da tempo, invero, in giurisprudenza si è enucleata la convinzione che nei reati associativi l'intercettazione sia possibile ovunque in risposta al clamore sociale che suscita tale tipologia di reati[184].

In sostanza, condivisibilmente con quanto sostenuto, con tale approdo, che si discosta non poco da quanto previsto dagli artt. 266 c.p.p. e 13 Cost., pare si confonda la tassatività *ratione loci* dei decreti ex artt. 266 c.p.p. e 13 Cost. con

---

[180] V., M.T. ABBAGNALE, *In tema di captatore informatico*, cit., 465.

[181] In questi termini, P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforme*, cit., 136.

[182] Cfr., in tal senso Cass. sez. un., 22 marzo 2005, n. 17706, in *Cass. pen.*, 2005, 2916 con nota a cura di G. MELILLO, *Appunti in tema di sospensione feriale dei termini relativi a procedimenti per reati di criminalità organizzata.*

[183] Come si nota il giudice di legittimità ha optato per una nozione di criminalità organizzata di tipo sostanzialistico che pone attenzione alla struttura organizzativa con i suoi requisiti di stabilità e di consapevolezza da parte degli asepti, ma anche alle finalità perseguite: una nozione ampia che trova il conforto della giurisprudenza europea. Per un approfondimento si rinvia a A. BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen.*, 2016, 2286.

[184] Cass. Sez. VI, 19 marzo 2013, n. 28602, in *Mass. Uff.* n. 256648.

la facoltà di eseguire le intercettazioni ovunque per i soli reati di criminalità organizzata.
In questo modo si confonde la *ratio* della captazione ambientale – ovvero il coinvolgimento o meno della privata dimora – con un elemento necessario dell'autorizzazione, posto che compete pur sempre al giudice individuare la relazione reato-luogo di intercettazione[185].
Se da un lato, l'art. 267 c.p.p. prevede che il giudice possa autorizzare l'intercettazione solo ove essa sia connotata dall'assoluta indispensabilità e l'art. 13 Cost. ne legittima l'uso solo ove essa sia necessaria per lo svolgimento delle indagini in relazione ad un delitto di criminalità organizzata, non si comprende come possa reputarsi adeguatamente motivato un decreto di autorizzazione che non individui preventivamente il luogo ove utilizzare lo strumento informatico abilitando la captazione di tutte le conversazioni che ivi si svolgeranno[186].

9. *Le nuove coordinate giuridiche per il virus spia previste nella legge delega.*

È difficile negare che di un intervento legislativo vi fosse davvero bisogno, soprattutto per riorganizzare la disciplina delle intercettazioni e della divulgazione delle conversazioni processualmente irrilevanti nonchè per dare dignità giuridica al nuovo strumento di intercettazione, il captatore informatico che attualmente esprime, ad un tempo, una elevata efficacia investigativa e una significativa insidiosità per la riservatezza del cittadino.
Difficile negare, inoltre, che il mandato riformatore del Parlamento si sia espresso in una formulazione normativa assai poco rigorosa, talvolta contenutisticamente incompiuta e disorganica da un punto di vista strutturale[187].
Prendiamo ad esempio la delicata problematica del regime di divulgabilità delle conversazioni captate: qui il limite maggiore dell'attuale normativa è quello di trattare le intercettazioni alla stregua di qualsiasi atto di indagine vietandone la pubblicazione sino a quando l'atto è coperto dal segreto (cioè sino a quando non è conoscibile dalla difesa); caduto il segreto, può esserne pubblicato il contenuto.

---

[185] Diffusamente, cfr., A. CISTERNA, *Spazio ed intercettazioni, una liaison tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite*, in *questa rivista*, 2016, 331 ss.
[186] Il tema è stato ampiamente approfondito da A. GAITO, S. FURFARO, *Le nuove intercettazioni "ambientali" tra diritto dei cittadini alla riservatezza ed esigenze disicurezza per la collettività*, cit., 318, i quali rilevano che il decreto che non contenga l'indicazione del luogo ove espletare l'intercettazione mediante il captatore deve considerarsi nulla per carenza di motivazione.
[187] Sulle novità introdotte dalla riforma, v., G. SPANGHER, *La riforma Orlando*, a cura di G. SPANGHER, Pisa, 2017, 11 e ss.

Un'impostazione, questa, che non ha fatto i conti con le peculiarità dell'intercettazione: una sorta di "idrovora fonica" che tutto indistintamente succhia[188].
Infatti, per consentire al giudice di selezionare (nel contraddittorio delle parti) ciò che è rilevante per l'accertamento dei fatti, tutti i risultati delle intercettazioni dovranno essere messi preventivamente a disposizione della difesa, ma in tal modo il segreto cade e tutte le notizie "captate" – come quelle ritenute irrilevanti -, divengono divulgabili.
La pubblicazione di notizie attinenti alla sfera più personale ed intima di soggetti a qualsiasi titolo finiti nella rete a strascico di una intercettazione, quindi, è operazione deprecabile ma, allo stato, legittima.
Invece, con riguardo all'uso dei virus spia va rilevato che l'ampiezza e la complessità del dibattito suscitato dell'utilizzo dei c.d. "trojan" – o se si preferisce captatori informatici -, unitamente al monito delle Sezioni Unite, ha indotto il legislatore a prevedere in un comma (art. 1 comma 84) della delega uno specifico punto (lett. e) avente ad oggetto la disciplina delle "intercettazioni di comunicazioni o conversazioni tra presenti mediante immissione di captatori informatici in dispositivi elettronici portatili".
Poiché un numero sempre maggiore di comunicazioni (numero destinato a crescere) avvengono con modalità criptate, tali da vanificare l'utilizzo di un'intercettazione con forme tradizionali, l'unica intercettazione efficace sarà quella effettuata a mezzo di virus o programmi similari, installati sul dispositivo nella disponibilità del soggetto intercettato; programmi con i quali è possibile monitorare, con modalità occulte ed in modo permanente, sia il flusso di comunicazioni riguardanti sistemi informatici o telematici, sia il contenuto, consentendo l'acquisizione, mediante copia, di dati presenti o futuri all'interno delle memorie di un dispositivo informatico[189].
Le indicazioni della delega - nel momento in cui troveranno sostanza in una specifica legge – imporranno, sicuramente, una rilettura del quadro delineato dalla Cassazione.
Ad oggi, il legislatore si è fatto espressamente carico solo di alcuni dei problemi evidenziati dalle recenti decisioni sul tema e delle perplessità espresse dalla dottrina, con particolare riguardo alla possibilità "indiscriminata" di cap-

[188] Sul tema delle intercettazioni telefoniche e sulla loro validità per prevenire ilcrimine, cfr., V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.*, 1973, 376.
[189] L. ANNUNZIATA, *Trojan di Stato: l'intervento delle Sezioni Unite non risolve le problematiche applicative connesse alla natura del captatore informatico*, in *Parola alla difesa*, 2016, 189.

tazione, anche in luoghi di privata dimora e in "assenza" del presupposto della commissione del reato.
In questo senso si è previsto che:
- il giudice deve indicare la necessità dei trojan ai fini delle indagini e che l'attivazione del microfono potrà avvenire solo in conseguenza di apposito comando inviato da remoto e non con il solo inserimento del captatore informatico, nel rispetto dei limiti stabiliti nel decreto autorizzativo del giudice;
- la registrazione audio deve essere avviata dalla polizia giudiziaria o dal personale incaricato ai sensi dell'articolo 348, comma 4, c.p.p., su indicazione della polizia giudiziaria operante la quale è tenuta a indicare l'ora di inizio e fine della registrazione, secondo circostanze da attestare nel verbale descrittivo delle modalità di effettuazione delle operazioni di cui all'articolo 268 del medesimo codice.
La previsione è in linea con le aspettative poiché è idonea ad assicurare il diritto di difesa in una fase in cui a questa si riserva sempre minor spazio.
Un'attività, quindi, che si può definire "a uomo presente"; pertanto, nonun'applicazione iniziale con conseguente indiscriminato utilizzo, ma un controllo da parte della polizia giudiziaria costante sul monitoraggio.
Inutile dire che tali indicazioni comportano, ove applicate, un dispendio di costi e di personale di straordinario rilievo e un elevato rischio che il soggetto intercettato (o qualcuno a lui vicino) possa percepire la presenza della polizia giudiziaria[190].
Allo stesso tempo, però, la completezza del verbale con la descrizione puntuale di tutte le attività effettuate, consente alla difesa la possibilità di controllare quanto effettivamente espletato.
Due ulteriori indicazioni hanno, poi, una specifica valenza tecnica.
In primo luogo, il trasferimento delle registrazioni dovrà essere effettuato "soltanto verso il server della Procura così da garantire originalità ed integrità delle registrazioni"; inoltre al termine della registrazione il captatore informatico dovrà essere disattivato e reso definitivamente inutilizzabile su indicazione del personale di polizia giudiziaria operante.
In questo caso, la *ratio* perseguita è quella di evitare che ci sia una soluzione di continuità nella "catena di custodia" dei dati informatici per cui non si è voluto correre il rischio che i captatori possano essere lasciati "disattivati", ma pronti ad essere resi nuovamente operativi sui device dei soggetti intercettati.

[190] Addirittura si corre il rischio che lo strumento invasivo possa recuperare informazioni da persone estranee. In questi termini si vedano le osservazioni di M. T. ABBAGNALE, *In tema di captatore informatico*, cit., 481.

Dovranno, inoltre, essere utilizzati soltanto programmi informatici conformi a determinati requisiti tecnici stabiliti con decreto ministeriale da emanarsi entro 30 giorni dalla data di entrata in vigore dei decreti legislativi menzionati dalla delega.
Qui un problema si pone: ad oggi, in verità, mancano regole idonee a garantire l'affidabilità e i requisiti che deve possedere l'operatore a cui viene affidato il delicato compito di fornire i programmi virus[191].
L'indicazione della delega prevede, inoltre, la necessità che si tenga "costantemente conto dell'evoluzione tecnica al fine di garantire che tale programma si limiti a effettuare le operazioni espressamente disposte secondo standard idonei di affidabilità tecnica, di sicurezza e di efficacia".
Il fatto che il legislatore, visti i tempi di obsolescenza tecnologica, abbia dato tali indicazioni al riguardo rappresenta certamente una scelta logica e condivisibile: resta, però, da capire come un decreto da emanare entro una specifica data possa tenere costantemente conto dell'evoluzione della tecnica.
Verosimilmente la volontà del legislatore era quella di prevedere una revisione delle indicazioni tecniche a mezzo di una emanazione periodica.
Un'ulteriore quesito si pone in relazione all'utilizzazione del captatore. La soluzione proposta dalle Sezioni Unite ha costituito una significativa limitazione all'utilizzo di tale strumento poichè ha escluso la possibilità di disporre in termini generali l'attività, con riguardo a quelle destinate a svolgersi in luoghi di privata dimora; la stessa decisione, tuttavia, è in qualche modo venuta incontro alle esigenze investigative, proponendo un'interpretazione estensiva del concetto di delitti in tema di criminalità organizzata non rigidamente declinato sul piano normativo.
In questo senso, l'uso di intercettazioni captate attraverso i virus è stato ritenuto legittimo nei procedimenti relativi alla criminalità organizzata, intendendosi per crimine organizzato non soltanto reati di mafia e terrorismo, ma tutti quelli facenti capo ad un'associazione per delinquere, correlata alle attività criminose più diverse.
Sul punto l'indicazione della delega, tuttavia, non è sintonica rispetto alle indicazioni della cassazione: il legislatore ha, invero, stabilito che l'attivazione del dispositivo potrà sempre essere ammessa nel caso in cui si proceda per i delitti di cui all'articolo 51, commi 3 bis e 3 quater, c.p.p. e, fuori da tali casi, nei luoghi di cui all'articolo 614 c.p. soltanto qualora ivi si stia svolgendo l'attività criminosa, nel rispetto dei requisiti di cui all'articolo 266, comma 1, c.p.p.

[191] M. T. ABBAGNALE, *In tema di captatore informatico*, cit., 470.

Come si nota, si è persa l'occasione di chiarire una volta per tutte la latitudine dell'interpretazione del concetto di criminalità organizzata e la sua estensione all'associazione per delinquere.
Una garanzia sul piano formale va, infine, ravvisata laddove si è stabilito che il decreto autorizzativo del giudice deve – parrebbe in ogni caso - indicare le ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini: certo, per un'attività altamente invasiva si sarebbe potuto pretendere una motivazione più pregnante che fosse stata, sicuramente, in grado di tutelare meglio i diritti coinvolti.

10. *La scelta legislativa e i problemi interpretativi irrisolti*. Ma così non è stato: infatti, il Governo, senza tener conto di quanto evidenziato dalla critica, ha approvato lo schema di decreto che attua la legge 103/2017 in materia di intercettazioni codificando (negli artt. 4 e ss.) la disciplina in tema di utilizzo dei *trojan*.
La scelta operata è stata chiara: limitare l'utilizzo di tale strumento invasivo, da un lato, e consentirlo senza limiti, dall'altro, solo per i reati di terrorismo e criminalità organizzata.
E' evidente che l'opzione scelta segue, in parte, le indicazioni e le scansioni della giurisprudenza: epperò, se da un lato, il rischio è quello di non consentire alle capacità investigative di stare al passo coi tempi, dall'altro, bisogna prendere atto che la riforma non ha affrontato e risolto i vari problemi che l'istituto pone, né ha cercato di disegnare un equilibrio tra le esigenze di garanzie dell'individuo coinvolto nell'indagine e quelle connesse alle indagini.
La conseguenza non è di poco rilievo, considerato che in questa materia i diritti coinvolti possono sempre essere messi in crisi dall'utilizzo troppo ampio o maldestro del virus: una disciplina che circoscrive l'ambito di operatività dello strumento invasivo, invece, non solo consente il rispetto delle garanzie costituzionali coinvolte ma si adegua alle *performance* richieste in ambito europeo senza sacrificare le esigenze investigative.
Nello specifico, lo schema di decreto interviene sull'articolo 266 c.p.p., integrandolo (previa l'aggiunta di un'ulteriore comma – 2 bis) per chiarire che l'uso del captatore informatico in dispositivi elettronici portatili è consentito, ai fini dell'intercettazione tra presenti in ambito domiciliare, soltanto se si procede per i delitti di cui all'art. 51, commi 3 *bis* e 3 *quater*, c.p.p.
Al di fuori di quest'ambito procedimentale, l'uso del virus soggiace, se attivato in luoghi di dimora privata o assimilabili, al limite costituito dal presupposto dello svolgimento in atto di attività criminosa.

Qui la *ratio* sottesa alla norma è chiara: il domicilio resta ambito di tutela privilegiato eccezion fatta se in esso si stia svolgendo un'attività criminosa.
In sintesi: l'attivazione del *malware* è sempre possibile, se si procede per reati di criminalità organizzata (cosa sono? Qual è il perimetro della locuzione), anche in luoghi di privata dimora: in tutti gli altri casi è ammesso in forma residuale, solo se è in corso un'attività criminosa.
Dunque, per utilizzare i virus nell'ipotesi di reati che siano non qualificati di criminalità organizzata o terrorismo il giudice dovrà motivare congruamente la sua scelta, indicando anche gli ambienti in cui l'intercettazione ambientale effettuata con questi mezzi può avvenire.
Infatti, al fine di dare attuazione alla previsione che impone che il controllo sul flusso di comunicazioni non avvenga con il solo inserimento del captatore, ma da remoto, secondo le indicazioni e nei limiti indicati nel decreto autorizzativo, il giudice dovrà non solo motivare in relazione alla particolare modalità di intercettazione prescelta, ma indicare anche gli ambienti in cui la stessa debba avvenire, secondo un verosimile progetto investigativo che implica l'individuazione, anche in forma indiretta, dei luoghi in cui si sposterà il dispositivo mobile controllato (nell'impossibilità di prevedere specificamente tutti gli spostamenti dell'apparecchio controllato).
Secondo la relazione di accompagnamento dello schema di decreto, la circostanza che tale modalità di intercettazione sia consentita per i delitti più gravi anche in ambienti di privata dimora, non pone i medesimi problemi di specificazione degli ambienti controllati tutte le volte che l'intercettazione sia consentita in ambito, in senso lato, domestico alla sola condizione che vi si stia svolgendo l'attività criminosa.
Una volta captata la conversazione, la trascrizione del suo contenuto sarà sottoposta agli stessi limiti previsti dallo schema di decreto per le intercettazioni, per così dire, ordinarie.
Rimarranno fuori da ogni trascrizione nei brogliacci della polizia giudiziaria le conversazioni intercettate ritenute irrilevanti ai fini della prova dei fatti per cui si indaga.
Il tema della irrilevanza si risolve (per lo più) nella fase delle indagini preliminari e, sin dall'inizio, il materiale è sottoposto ad una valutazione di rilevanza o meno (ai fini della trascrizione) ad iniziare dalla polizia giudiziaria che, in caso di dubbio, si rivolgerà al pubblico ministero.
Il decreto, infine, disciplina una procedura che può essere sintetizzata in due distinte fasi (deposito dei brogliacci e acquisizione delle trascrizioni rilevanti) e che permetterà di individuare – nel contraddittorio tra pubblico ministero e difensori – le conversazioni rilevanti ai fini della prova: la parte restante e cioè

le registrazioni e le annotazioni del luogo, della data e dell' ora della intercettazione finirà in un archivio riservato così come specificatamente previsto dal nuovo art. 89 *bis* disp att. c.p.p.
In questo modo, nello spirito del legislatore, viene garantita la tutela della *privacy* di quelle persone che sono estranee alla vicenda investigativa.
Ma, il vero vizio di fondo dell'intera riforma sta nel fatto che il virus viene considerato solo alla stessa stregua di un'intercettazione.
In realtà esso non lo è o, per lo meno, si configura come un'intercettazione "anomala" che, di fatto, opera su più fronti: come un'ispezione o una perquisizione attraverso cui si individua il dato o l'informazione da recuperare all'insaputa del destinatario e senza il rispetto delle garanzie che ad esso sono dovute, e come un meccanismo di estrapolazione dei dati informatici anche protetti o cancellati alla stregua di un accertamento tecnico, alle volte addirittura irripetibile, effettuato all'insaputa dell'interessato e nel disinteresse completo delle sue prerogative difensive.
Va, infatti, osservato che la legge Orlando ha circoscritto l'attenzione solo su una delle molteplici potenzialità di azione di questo *malicions software*, ossia il suo utilizzo quale strumento per l'esecuzione di intercettazioni di comunicazioni tra presenti, di videoripresa e di intercettazione di flussi telematici, trascurando completamente di affrontare le questioni giuridiche connesse alle altre attività che possono essere eseguite dal virus e che consentono all'organo inquirente di accedere a tutto il contenuto del *device* infettato: immagini, file, email, video, dati informatici, rubriche, ecc[192].
Il virus, invero, essendo in grado di invadere ogni parte del dispositivo e, quindi, di acquisire ogni tipo di informazione in esso contenuta, finisce, di fatto, per trasformarsi in una perquisizione informatica a cui segue l'apprensione del contenuto (cioè il suo sequestro); inoltre, operando al di fuori dello schema tipico di un'intercettazione o di una perquisizione (si pensi alla distruzione e sostituzione di *files*, all'invio di comunicazioni o all'installazione di programmi ulteriori), pone ulteriori problemi di garanzie[193].
Problemi, questi ultimi, che valgono anche con riferimento alla modifica operata sull'art. 89 disp. att. c.p.p. ove è stato precisato che quando si procede con l'utilizzo del captatore il verbale deve indicare il tipo di programma che viene utilizzato e che possono essere impiegati soltanto programmi che siano conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia.

[192] In tema, E. TURCO, *La ricerca della prova ad alta efficacia intrusiva: il captatore elettronico*, in *La riforma della giustizia penale*, a cura di A. SCALFATI, Milano, 2017, 311.
[193] In questi termini, cfr., E. TURCO, *La ricerca della prova ad alta efficacia intrusiva: il captatore elettronico*, in *La riforma della giustizia penale*, cit., 311.

Anche in questo caso il *vulnus* è evidente: il legislatore, ancora una volta, non ha specificato quali siano le garanzie a tutela della bontà dei programmi e che requisiti debba avere colui che deve garantire tale bontà.
Un ulteriore chiarimento auspicabile riguarda la nozione di criminalità organizzata e la sua esatta perimetrazione. Ancora una volta, il tema è rimasto sullo sfondo, lasciando il concetto ancorato alla vecchia interpretazione giurisprudenziale e non alle esigenze di limitare la maggiore invasività solo a quelle situazioni nelle quali il peculiare controllo del territorio rende il fenomeno criminale particolarmente pericoloso e degno del c.d. doppio binario (declinazione troppo ampia per essere riferita a fatti eccezionali).
Un'occasione mancata, dunque, per intervenire anche su tali aspetti peculiari: una lacuna ingiustificabile e particolarmente allarmante, perché lascia i cittadini senza alcuna tutela di fronte all'enorme potenzialità invasiva e pervasiva di tale "*bulimico*" congegno che, inesorabilmente, finisce per rendere vani i diritti difensivi e ignorare i divieti probatori fissati dalla legge[194].
Il tutto senza considerare, infine, che il captatore, comunque, presenta indubbi fattori di criticita: basti pensare che il *software* non si attiva se l'utente è particolarmente scaltro o prudente e, quindi, omette di cliccare sul *link* inviato dall'organo inquirente ovvero non apre i *files* provenienti dall'esterno.

[194] L'espressione è di L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante: le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, cit., 350.