ALESSANDRA SCALAS

I confini mobili della *digital evidence*: una necessaria tassonomia per la tutela delle garanzie

L'indagine sulla digital evidence restituisce un quadro frammentario, privo di regolamentazione specifica. L'incalzante esigenza di adeguare le forme processuali all'era tecnologica impone di ripensare le categorie sistemiche per consentire l'ingresso e l'utilizzo di materiale probatorio sui generis, senza però trascurare le ricadute sui diritti fondamentali dell'individuo.

The shifting boundaries of digital evidence: a necessary taxonomy for the protection of warranties

The framework pertaining to digital evidence *results to be fragmentary and unregulated. The pressing need to adapt procedural forms to the digital age requires us to rethink systemic categories in order to admit and utilize non-standard evidence, always keeping close attention to the fundamental rights of the individual.*

1. *Premessa.* Nonostante l'impatto delle nuove tecnologie sulle strutture processuali sia ormai innegabile, il percorso di adeguamento a nuovi modelli si rivela lento e graduale[1] e tutt'altro che lineare. L'interprete è così chiamato a destreggiarsi tra l'esigenza di modernizzazione, connaturata alla società stessa, e la salvaguardia delle garanzie dei soggetti coinvolti nelle vicende giudiziarie.
La questione pone un interrogativo di fondo: quanto in là può spingersi la macchina della giustizia per accertare la verità processuale?
L'ausilio delle nuove tecnologie contribuisce a rafforzare la soglia di certezza[2], garantendo una più efficace applicazione delle regole di giudizio, ciò, tuttavia, non può tradursi in una indiscriminata invasione nella sfera personale del singolo nell'ottica del risultato.
E se il risparmio di formalismi è sicuramente proficuo, giacché il principio di ragionevole durata del processo[3] ha matrice costituzionale (art. 111, co. 2

[1] Cfr. LORUSSO, *Digital evidence, cybercrime e giustizia penale 2.0*, in *Proc. pen. giust.*, 2018.
[2] Giova tuttavia precisare che con riferimento alla prova digitale non bisogna commettere l'errore di fraintenderne il valore probatorio, giacché essa non è perfettamente sovrapponibile alla prova perfetta. In argomento v. PITTIRUTI, *Digital evidence e procedimento penale*, 2017, 15.
[3] La concreta attuazione del principio costituisce uno dei fili conduttori della riforma Cartabia. CORETTI, *La ragionevole durata delle indagini alla luce della riforma Cartabia: nihil sub (italico) sole novum*, in *questa Rivista*, 2022, 2, 3, puntualizza che la lentezza della macchina giudiziaria italiana condiziona negativamente la percezione della qualità della giustizia ponendo interrogativi sulla tenuta dello stato di diritto.

Cost.) e convenzionale (art. 6, par. 1 C.E.D.U.), altrettanto non può ritenernesi per quelle forme del procedere poste a tutela dei diritti fondamentali[4].
La mancata perimetrazione normativa della c.d. *digital evidence*[5] impone uno sforzo notevole nel ricondurre a quella o ad altra categoria la congerie di elementi probatori attinti dai dispositivi elettronici. Non stupisce allora che, in presenza di confini mobili, anche la Cassazione si muova tra le intersezioni normative nel tentativo di evitare la dispersione di prove dirimenti, anche in chiave deflattiva.

2. *Digital evidence: una questione meramente classificatoria?* Le interazioni tra le scienze informatiche e telematiche ed il processo penale incidono sul sapere giuridico processuale sotto il profilo quantitativo e qualitativo[6]. D'altronde, nell'era moderna il ricorso a strumenti informatici e telematici mediante i quali trasmettere e ricevere informazioni risulta ormai imprescindibile, avendo quasi sostituito del tutto modalità più obsolescenti di comunicazione; l'avanzamento del digitale influenza il vivere sociale[7] al punto da condizionarne ogni aspetto, incluse le regole volte all'accertamento dei fatti di reato[8]. Tale apporto si concretizza sotto forma di creazione di nuovi strumenti investigativi e di nuove tipologie di prove[9] , essendosi affermata l'esigenza di ricercare «elementi di prova tra i dati contenuti in sistemi informatici o telematici»[10]. Invero, tali dispositivi possono rappresentare il mezzo per commet-

[4] Né tuttavia si può ammettere «che l'incontrollata proliferazione delle "garanzie difensive" finisca di fatto per paralizzare il corso dei processi», FERRUA, *La ragionevole durata del processo tra Costituzione e Convenzione europea*, in *Quest. giust.*, 2017, 1, 110.
[5] Come accuratamente precisato da MARAFIOTI, *Digital evidence e processo penale*, *Relazione al Convegno "Prova penale e attualità controverse", organizzato dal Consiglio dell'Ordine degli Avvocati di Roma*, in *Cass. Pen.*, 2011 12, 4510, la *digital evidence* rischia di essere compromessa o distrutta, seppur involontariamente, da personale privo delle adeguate conoscenze. Ciò è ancor più grave in virtù del fatto che «la partita si gioca essenzialmente fuori dal dibattimento, durante le indagini preliminari; e sono in gioco interessi rilevantissimi, costituzionalmente garantiti, come il diritto di difesa».
[6] Così, PITTIRUTI, *Digital evidence e procedimento penale*, 2017, 2.
[7] CUOMO-GIORDANO, *Informatica e processo penale*, in *Proc. pen. giust.*, 2018; in argomento v. GIUNCHEDI, *Le malpractices nella digital forensics*, in *questa Rivista.*, 2013, 3, 821.
[8] PITTIRUTI, *op. cit.*, 1. V. anche DI CHIARA, *Il canto delle sirene. Processo penale e modernità scientificotecnologica: prova dichiarativa e diagnostica della verità*, in *Criminalia*, 2007, 19 ss.
[9] Cfr. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. Pen.*, 2015, 760 ss.; PITTIRUTI, *op. cit.*, 1
[10] PITTIRUTI, *op. cit., 2; ex multis* in argomento *v.* LUPARIA, *La disciplina processuale e le garanzie difensive*, in *Investigazione penale e tecnologia informatica*, a cura di Luparia- Ziccardi, Milano, 2007,

tere reati, contenere le prove dei crimini comuni, rappresentare l'obiettivo di illeciti[11].

La prova informatica[12] è strettamente legata alla fase delle investigazioni[13], che possono risultare al punto intrusive da rivelare molto della vita di un individuo, anche gli aspetti più privati[14]. A venire in rilievo sono i diritti inviolabili dell'uomo, come la libertà, la segretezza[15] della corrispondenza e l'inviolabilità del domicilio riconosciuti e sanciti dalla Carta costituzionale e ribaditi a livello europeo ed internazionale[16].

Uno dei profili più controversi è proprio la tutela della *privacy* dei soggetti[17], fortemente a rischio per l'impiego di siffatte tecnologie.

---

127 ss.; COLAIOCCO, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria,* in *questa Rivista.,* 2019, 1, 1.

[11] Cfr. CUOMO- GIORDANO, *op. cit.*

[12] In argomento v. SANNA, *La prova informatica al vaglio del giudice, tra cattiva scienza e cattivi scienziati*, in *Discrimen*, 2022; DI PAOLO, voce *Prova informatica (diritto processuale penale)*, in *Enc. dir., Annali*, VI, Milano, 2013.

[13] Così GUALTIERI, *Prova informatica e diritto di difesa*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, 70; cit. ripresa da PITTIRUTI, *op. cit.,* 2

[14] CONTI - TORRE, *op. cit.*, 562.

[15] È da sottolineare la genesi della materia del trattamento dei dati personali si è avuta con la legge 21 febbraio 1989, n. 98 che ratificava la Convenzione di Strasburgo n. 108 del 28 gennaio 1981. In argomento v. TRONCONE, *La rilevanza penale del trattamento dei dati personali*, in *questa Rivista*, 2021, 1, 7; MILITELLO, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. econ.*, 1992. PECORELLA, *Il diritto penale dell'informatica*, Padova, 2000.

[16] Va, tuttavia, precisato che una possibile deroga ai fini di accertamento e prevenzione del crimine è ammessa sulla base della riserva di legge e di giurisdizione. Peraltro, analoga riserva di legge è prevista a livello convenzionale dall'art. 8 C.E.D.U. SCACCIANOCE, *op. cit.* 105. Inoltre, va debitamente tenuto conto che la disciplina che prevede che un atto possa limitare i diritti fondamentali dev'essere sempre ispirata al principio di proporzionalità: non solo la misura limitativa dev'essere in grado di raggiungere lo scopo e risultare indispensabile per esso, ma il sacrificio imposto al bene deve ritenersi giustificato sulla base della gravità del reato contestato. CONTI-TORRE, *op. cit.*, 536.
Recentemente, la Corte di cassazione (Cass., Sez. II, 13 febbraio 2020, n. 5741, Rv. 278568) ha puntualizzato che in tema di acquisizione di dati contenuti in tabulati telefonici, la disciplina italiana di conservazione dei dati di traffico c.d. "*data retention*" – di cui all'art. 132, d. lgs 30 giugno 2003, n. 196, è compatibile con le direttive n. 2002/58/CE e 2006/24/CE in tema di tutela della "privacy", come interpretate dalla giurisprudenza della Corte di giustizia dell'U.E. (C.G.U.E. 8 aprile 2014, *Digital Rights*, C-293/12 e C-594/12; C.G.U.E. 21 dicembre 2016, Tele 2, C-203/15 e C-698/15), poiché la deroga stabilita dalla norma alla riservatezza delle comunicazioni è prevista per un periodo di tempo limitato, ha come esclusivo obiettivo l'accertamento e la repressione dei reati ed è subordinata alla emissione di un provvedimento da parte di un'autorità giurisdizionale.

[17] Al tema si ricollega anche una recente pronuncia della Corte di giustizia dell'U.E. su un rinvio pregiudiziale, sentenza 29 luglio 2019, concernente l'interpretazione degli articoli 2, 7, 10, da 22 a 24 della direttiva 95/46/CE (abrogata e sostituita, a decorrere dal 25 maggio 2018, dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016) del Parlamento europeo e del

La tematica ha assunto sempre più risonanza a livello europeo[18], portando all'emanazione del cd. "Pacchetto protezione dati" U.E. riferibile a quegli atti normativi di matrice comunitaria relativi al trattamento, la protezione e la libera circolazione dei dati personali e «volti a rispondere alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica [...]»[19]. Quest'ultimo si compone del Regolamento (UE) 2016/679[20] del Parlamento europeo e del Consiglio, del 27 aprile 2016, entrato in vigore in tutta l'Unione Europea il 25 maggio 2018, che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati); nonché della Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, attuata mediante il d. lgs. 51/2018[21]. Si è infatti avvertita l'esigenza nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia di stabilire norme specifiche sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica, nel rispetto della na-

---

Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Tale domanda viene presentata nell'ambito di una controversia tra la *Fashion ID GmbH & Co. KG* e la *Verbraucherzentrale NRW eV* in ordine all'inserimento, da parte della *Fashion ID*, di un *plug-in social* della *Facebook Ireland Ltd* nel proprio sito internet. Consultabile in *https://www.eius.it/giurisprudenza/*.

[18] Per un approfondimento sul tema dell'accesso transfrontaliero alla prova digitale, si veda TONDI, *L'accesso transfrontaliero all'electronic evidence, tra esigenze di effettività e tutela dei diritti*, in *Dir. pen. cont.*, 2019, 2. In argomento v. anche CONTI, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica e diritto*, XLI annata, 2015, 1-2, 161, che sottolinea che «con la Direttiva 2014/4 [...] viene creato un «sistema globale di acquisizione delle prove nelle fattispecie aventi dimensione transfrontaliera»: con l'ordine europeo di indagine lo Stato di emissione ottiene che venga compiuto in un altro Stato membro (c.d. di esecuzione) un determinato atto di indagine senza che siano necessarie ulteriori formalità e in modo veloce ed efficace».

[19] *Temi Camera dei deputati, Giustizia, Protezione dei dati personali.*, in *https://temi.camera.it/leg19DIL/temi/protezione-dati-personali*.

[20] Così TRONCONE, *op. cit.*, 7, che precisa che «il Regolamento prevede nel suo apparato sanzionatorio la punibilità unicamente degli illeciti amministrativi, non esiste alcuna previsione di fattispecie penali». L'autore sottolinea che probabilmente «la scelta è stata indotta dal fatto che negli stati nazionali il principio generalmente vigente in materia penale è quello della riserva di legge e dove vige la garanzia di fonte alta della stretta legalità per cui può intervenire a legiferare norme repressive soltanto il Parlamento di quel paese».

[21] In particolare, si tratta di un testo unitario, che disciplina complessivamente il trattamento di dati personali in ambito penale, prevedendo sia principi generali che disposizioni di dettaglio di diversi settori che concernono il trattamento dei dati personali. *Temi Camera dei deputati, Giustizia, Protezione dei dati personali.*, in *https://temi.camera.it/leg19DIL/temi/protezione-dati-personali*.

tura specifica di tali attività[22]. In effetti, è solo con il decreto legislativo 101/2018[23] che si realizza l'armonizzazione delle norme contenute nel Codice in materia di protezione dei dati personali (D.Lgs. 196/2003)[24] con quelle introdotte dal Regolamento Europeo 2016/679. È da precisare, infatti, che la Direttiva (UE) 2016/680, ha natura di *lex specialis* rispetto al regolamento generale sulla protezione dei dati, giacché ne attua i princìpi e gli obblighi con riferimento alle attività e ai poteri delle autorità di polizia e giudiziarie[25].
Inoltre, dal 2017 la Commissione europea ha avviato la revisione della disciplina concernente la tutela della riservatezza delle comunicazioni elettroniche al fine di adeguarla agli *standard* di protezione previsti dal pacchetto protezione dati, nonché per renderla «tecnologicamente neutra rispetto alla continua evoluzione delle tecnologie in materia di comunicazione e informazione»[26].
Sul versante prettamente processuale, si è assistito ad un gradato adeguamento agli *input* sovranazionali[27] – attraverso la modifica di diverse disposizioni del codice di rito penale – mediante l'introduzione delle c.d. "*best practices*":

---

[22] Così CARRER, *Privacy e diritto penale: approvato in via definitiva il d. lgs. 51/2018 che attua la direttiva europea sulla tutela dei dati personali a fini di pubblica sicurezza e penali*, in *Giur. pen. web*, 2018.
[23] Sul tema si veda D'AGOSTINO, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101*, in *questa Rivista*, 2019, 1, 1 ss.
[24] Novellato con l'intervento del d.l. 139 del 2021, convertito con modificazioni dalla L. 3 dicembre 2021, n. 205 (in G.U. 7/12/2021, n. 291), che ha apportato modifiche a diverse disposizioni in materia di protezione dei dati personali. Da ultimo, con l'intervento del D.Lgs. 10 marzo 2023, n. 24, con effetto a decorrere dal 15 luglio 2023.
[25] *Temi Camera dei deputati, Giustizia, Protezione dei dati personali.*, in *https://temi.camera.it/leg19DIL/temi/protezione-dati-personali.*.
[26] Cfr. *supra.* In particolare, è stata presentata una proposta di regolamento COM (2017)10 volta a sostituire la direttiva 2002/58/CE (cosiddetta e-privacy) con una normativa che sia direttamente applicabile e che assicuri i medesimi livelli di protezione per tutti i cittadini UE utenti delle comunicazioni elettroniche. Inoltre, con riferimento alla materia dei dati non personali si segnalano il Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio; Comunicazione della Commissione al Parlamento europeo e al Consiglio del 29 maggio 2019 (COM (2019) 250) recante le Linee guida sul regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.
[27] COLAIOCCO, *op. cit.,* 2. Sul tema v. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008; ATERNO, *La Convenzione di Budapest del 2001 e la L. n. 48/2008*, in *Cybercrime*, a cura di Cadoppi – Canestrari – Manna - Papa, Utet, Torino, 2019, 1351 ss.; CORDÌ, *Sub art. 8 l. 18.3.2008 n. 48*, in *Leg. pen.*, 2008, 282 ss.; DI BITONTO, *L'accertamento investigativo delle indagini sui reati informatici*, in *Dir. internet*, 2008, 503 ss.; LUPARIA, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. I profili processuali*, in *Dir. pen. proc.*, 2008, 717 ss.; CONTI, *op. cit.,* 154 ss. Da ultimo si veda *Criminalità informatica: siglato il secondo protocollo*, in *Dir. giust.*, 2022, con riferimento al contenuto del secondo protocollo alla Convenzione di Budapest sulla criminalità informatica.

comportamenti da seguire per l'effettuazione di operazioni informatiche su dispositivi o supporti, evidenziando la necessità di preservare le tracce del procedimento di raccolta di *digital evidence* mediante *report* allo scopo di evitare potenziali alterazioni del dato digitale in sede di ammissione della prova[28]. Si vuole così garantire alle parti l'esperimento di indagini e consulenze su un dato «che risulta genuino e perfettamente cristallizzato»[29].
Resta, però, insoluta la questione classificatoria[30], non essendovi univocità di vedute sull'inquadramento dogmatico della prova informatica.
È da premettere che, da un punto di vista tecnico, con *digital forensics* si intende l'evoluzione della *computer forensics*[31]. Invero, lo scopo di quest'ultima era il recupero dei dati persi o cancellati da file; diversamente, la prima si occupa non solo del recupero dei dati, ma del conseguente adattamento al contesto giuridico consentendone la ripetibilità nel procedimento penale[32].
Taluni ricorrono alla nozione di *digital evidence* – mutuata dalla disciplina statunitense – come definizione generica per alludere ad una serie di «strumenti investigativi e probatori suscitati e alimentati dalla rivoluzione informatica»[33]. L'espressione, in alcuni casi, è tradotta come "prova digitale", facendo

[28] Sul punto diffusamente v. COLAIOCCO, *op. cit.,* 2, che precisa che si tiene traccia del procedimento di raccolta attraverso la preservazione della *chain custody.* In argomento anche GIUNCHEDI, *op. cit.*, 826; TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48,* in *Informatica e diritto,* XLI annata, Vol. XXIV, 2015, 1-2, 74 ss.
[29] Così GIUNCHEDI, *op. cit.*, 826. L'Autore precisa che l'adozione di protocolli operativi (S.O.P) riduce notevolmente i rischi, consentendo di applicare la miglior tecnica al momento disponibile, giacché l'irripetibilità del dato digitale non ammette errori, pena lo smarrimento del patrimonio conoscitivo in essi contenuto. V. anche ID*, Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, Torino, 2009, *passim.*
[30] PITTIRUTI, *op. cit.,* 6.
[31] Più propriamente intesa come quell'ambito di ricerca che si occupa delle problematiche tecniche e giuridiche connesse alle investigazioni sui dati digitali. Così PITTIRUTI, *op. cit.*, 3.
[32] Così GIUNCHEDI, *op. cit.*, 824, che precisa che «è oramai pacifico che per ottenere risultati giuridicamente plausibili occorre utilizzare metodologie che traggono origine dalla scienza, com'è da considerare a tutti gli effetti la *digital forensics*». V. anche, *Le indagini sui reperti invisibili.* High tech crime, in *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze*, a cura di Curtotti - Saravo, Torino, 2013, 709; PETERSON - SHENOI, *Advances in digital forensics V*, (*IFIP International Federation for Information Processing*), 2009.
[33] LORUSSO, *Digital evidence, cybercrime e giustizia penale 2.0,* in *Proc. pen. giust.*, 2018. L'espressione è linea con la disciplina internazionale.

leva sul «dato, frutto di una manipolazione elettronica di numeri»[34]; altri, hanno ritenuto preferibile discorrere di "prova di natura digitale"[35].
Altri ancora utilizzano indistintamente, come sinonimi, le locuzioni «prova digitale», «prova elettronica», «prova informatica»[36]. Ebbene, è proprio la natura proteiforme del dato digitale che non consente di circoscrivere il fenomeno della *digital evidence* all'interno di confini ben precisi. I profili critici involgono sia la metodologia di reperimento del dato digitale, giacché va tenuto in debito conto lo strumento da cui viene tratto, sia il risultato di prova che è variamente classificabile[37].
Nell'indagine ricostruttiva la prova digitale è stata assimilata alla prova scientifica[38], in virtù del tasso elevato di tecnicismo richiesto per rendere fruibili per il giudice informazioni contenute in macchinari complessi[39]. Quest'ultima è stata recentemente oggetto d'interesse del legislatore[40], che ha ridefinito i contorni della *nuova* prova scientifica[41], intesa come «mezzo probatorio nel quale s'impiega uno strumento di prova scientifico tecnico nuovo o controverso e di elevata specializzazione»[42].
La giurisprudenza più recente ha precisato che «in tema di prova scientifica, il giudizio di attendibilità di una teoria deve tener conto degli studi che la sorreggono e delle basi fattuali sui quali sono condotti, dell'ampiezza, della rigorosità e dell'oggettività della ricerca, del grado di sostegno che i fatti accordano alla tesi, della discussione critica che ha accompagnato l'elaborazione dello studio e delle opinioni dissonanti che si siano eventualmente formate, dell'at-

[34] Così PITTIRUTI, *op. cit.*, 7. V. anche DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.* 2011, 283; ID, *Caratteristiche della prova digitale*, in *Nuove tendenze della giustizia penale di fronte alla criminalità informatica: aspetti sostanziali e processuali*, a cura di Ruggeri - Picotti, Torino, 2011, 204.
[35] PITTIRUTI, *op. cit.*, 7; MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. Pen.*, 2013, 1261.
[36] PITTIRUTI, *op. cit. 8.* V. sul punto DI PAOLO, *voce Prova informatica (diritto processuale penale)*, in *Enc. Dir., Annali*, VI, Milano, 2013, 736.
[37] PITTIRUTI, *op. cit.*, 8
[38] Così, MANCUSO, *op. cit.,* 504. In argomento *ex multis* v. MARCOLINI, *op. cit.,* 700; DOMINIONI, v*oce Prova scientifica (diritto processuale penale)*, in *Enc. Dir., Annali*, II, Milano 2008; CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. Pen.*, 2008, 3520; CECCHI, *Il giudice dinanzi alla prova scientifica*, in *questa Rivista,* 2022, 1.
[39] MARAFIOTI, *Digital evidence e processo penale*, *Relazione al Convegno "Prova penale e attualità controverse", organizzato dal Consiglio dell'Ordine degli Avvocati di Roma*, in *Cass. Pen.*, 2011, 12, 4510.
[40] Si fa riferimento all'avvento della Riforma Cartabia, attutata mediante il d.lgs. 150/2022.
[41] In argomento V. Relazione Ufficio del Massimario, 2023, 2, 127 ss.
[42] DOMINIONI, *Il diritto delle prove*, in *Procedura penale*, a cura di AA.VV., Torino, 2023, 308.

titudine esplicativa dell'elaborazione teorica, del grado di consenso che la tesi raccoglie nella comunità scientifica, nonché dell'autorità e dell'indipendenza di chi ha effettuato la ricerca»[43]. Il collegamento con la prova digitale è presto detto: l'attività che riguarda l'informatica forense va ben oltre le competenze basiche, richiedendo conoscenze tecniche e specializzate.

Tuttavia, non bisogna commettere l'errore di perdere di vista le diversità ontologiche in quanto le peculiarità della prova scientifica emergono in fase di ammissione, assunzione e valutazione della prova; nel caso di prova digitale il ricorso a strumentazione specializzata è richiesto già in fase di ricerca e raccolta dell'informazione, cioè in fase investigativa, affinché converga all'interno del procedimento e, poi, per l'analisi del dato[44].

Soltanto dalla collocazione topografica può discendere l'applicazione di regole ben precise.

Al riguardo, si è tentato di sgombrare il campo da difficoltà interpretative riconducendo la prova digitale al paradigma della prova atipica *ex* art. 189[45] c.p.p., che rispecchia la scelta legislativa di non impedire aprioristicamente l'ingresso nel processo di prove non disciplinate dalla legge, rimettendo al giudice il compito di una valutazione in concreto sull'ammissibilità (purché non si tratti di prove vietate dalla legge o difformi per qualche difetto della fattispecie dal modello di una prova tipica)[46]. Eppure, tale ipotesi è stata posta in discussione sulla base di un duplice ordine di ragioni: in primo luogo, l'intervento della legge 48/2008, che ha operato modifiche al codice di rito penale, ridisegnando i confini di alcuni istituti per adattarli alle nuove sfide tecnologiche (*rectius*: alle problematiche concernenti la *digital evidence*). Inoltre, proprio con riferimento al richiamato modello di prova scientifica si è

[43] Cass., Sez. V, 17 gennaio, 2022, n. 1801, Rv. 282545.

[44] PITTIRUTI, *op. cit.*,15. Peraltro, l'autore si diffonde in maniera minuziosa sui punti di convergenza e divergenza tra le due "tipologie" di prove, evidenziandone i profili critici.

[45] Ritenuta, in taluni casi, come elemento distonico rispetto all'impostazione legislativa. Difatti, alla luce del principio di legalità e proporzionalità, «il volto in negativo del quadro [...] è quello della prova incostituzionale: quando non esiste una norma di rango legislativo che soddisfi – nell'*an* e nel *quomodo* – la predetta riserva, l'acquisizione non può che considerarsi vietata; dal silenzio del legislatore si ricava un limite probatorio. Come si è accennato, in presenza di un divieto la strada maestra è già chiara: qualora il confine sia oltrepassato si intravede il volto implacabile dell'inutilizzabilità ex art. 191 c.p.p.». Così, CONTI - TORRE, *Spionaggio digitale nell'ambito dei social network*, in *Le indagini atipiche*, a cura di Scalfati, Torino, 536. In argomento v. MARCOLINI, *voce Prove atipiche (diritto processuale penale)*, in *Enc. Dir., Annali*, X, Milano, 2017. Più nel dettaglio si veda MARAFIOTI, *op. cit.*, 4510.

[46] GREVI - ILLUMINATI, *Prove*, in *Compendio di procedura penale*, a cura di Conso - Grevi - Bargis, 2020, 268.

sostenuto che, da un lato, essa si configura come diversa manifestazione di istituti preesistenti; dall'altro, si è ritenuto che il sistema disponga già di strumenti adeguati (perizia, consulenza tecnica) per garantire l'ingresso di prove tecnico-scientifiche. Applicando tali considerazioni alla prova informatica – intesa come *digital evidence* – verrebbe meno la necessità di ricorrere al modello di prova atipica[47]. Va però precisato che, in realtà, la giurisprudenza ha ribadito l'appartenenza alla categoria di cui al 189 c.p.p. di quelle indagini che non ricalchino il paradigma legale[48].

Si discorre, infatti, di mezzi di ricerca della prova atipici, così come riconosciuti dalla Cassazione[49]. Il punto di frizione, però, è la potenziale compromissione delle garanzie del singolo, se si considera che con la locuzione prova digitale si allude ad una molteplicità di situazioni dagli ampi risvolti quanto all'apprensione dei dati raccolti anche in modi diversi.

Dubbi ermeneutici sorgono anche con riferimento alla c.d. prova "algoritmica", che risulta *species* del *genus* della prova scientifica informatica; se, tuttavia, con riferimento alla *digital evidence* è indispensabile l'intervento dell'uomo per la raccolta dell'elemento probatorio, nel caso dell'*automated*

---

[47] In argomento, in maniera approfondita, vedi PITTIRUTI, *op. cit.*, 20, il quale evidenzia che, *prima facie*, il modello della prova atipica di cui all'art. 189 c.p.p. si rivela intrinsecamente incompatibile con lo svolgimento di una attività investigativa sul dato digitale che, per avere riscontri, dovrebbe rimanere segreta. Invero, un contraddittorio preventivo potrebbe minare tale prerogativa.

[48] Cass., Sez. II, 21 maggio 2013, n. 21644, Rv. 255542. La Corte ha precisato che «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 seguenti cod. proc. pen.; 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 senso conforme, da ultimo, Cass., Sez. IV, 07 giugno 2022, n. 21856, Rv. 283386.

[49] Cass., Sez. VI, 12 aprile 2023, n. 15422, Rv. 284582, da ultimo ha precisato che «la localizzazione degli spostamenti tramite sistema di rilevamento satellitare GPS (c.d. pedinamento elettronico) è mezzo di ricerca della prova atipico non implicante un accumulo massivo di dati sensibili da parte del gestore del servizio, sicché le relative risultanze sono utilizzabili senza necessità di autorizzazione da parte dell'autorità giudiziaria, non trovando applicazione per analogia la disciplina di cui all'art. 132, comma 3, d.lgs. 30 giugno 2003, n. 196 e successive modifiche, in tema di tabulati, e neppure i principi affermati dalla sentenza della C.G.U.E. del 05/04/2022, C. 140/2020, relativa alla compatibilità di "*data retention*" con le Direttive 2002/58/CE e 2009/136/CE, sul trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni».

Più in generale sul tema dei mezzi di ricerca della prova sorti in conseguenza delle innovazioni tecnologiche v. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *questa Rivista*, 2014, 1.

evidence il processo è del tutto automatizzato grazie all'intelligenza artificiale. Sicché, sarebbe auspicabile un vaglio preliminare sulla qualità degli elementi così raccolti e una qualificazione probatoria indiziaria ogniqualvolta il giudice[50] non riesca a comprendere l'algoritmo che ha consentito al *software* di raccogliere e valutare il dato[51].

L'esigenza di tutela dei diritti fondamentali dell'individuo si fa ancor più incalzante col ricorso agli algoritmi informatici, soprattutto durante la fase delle indagini. In ambito processualpenalistico l'intelligenza artificiale[52] è di ausilio alla polizia per molteplici scopi, tant'è che si discorre delle attività di 'polizia predittiva', che si sostanziano nello studio e nell'approfondimento di dati ed informazioni riguardanti la commissione di determinati reati, nonché nell'applicazione di procedure e modelli statistici che consentono di prevedere, prima del fatto stesso, le circostanze di tempo e luogo ove questo potrebbe avere esecuzione, sinanche l'autore[53]. È indubitabile che nel processo transitino sempre più di frequente elementi attinti mediante le tecnologie intelligenti.

---

[50] SACCOMANI, *L'impatto della giustizia algoritmica sul diritto all'equo processo*, in *Cass. Pen.*, 2023, 2, 631-632, precisa che riveste particolare importanza il «diritto di accedere all'algoritmo, al fine di comprendere la sua logica ed il suo funzionamento. Tale conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti, fornendo adeguate informazioni sui suoi autori, sul procedimento usato per la sua elaborazione, sul meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e sui dati selezionati come rilevanti. Quanto sopra si rende necessario al fine di poter effettuare delle verifiche circa gli esiti del procedimento robotizzato e della loro conformità alle prescrizioni ed alle finalità stabilite dalla legge»

[51] MAGLIULO, *L'Intelligenza Artificiale nel processo penale: progresso o rischio per la tutela dei diritti costituzionali?, in Il Processo,* 2022, 2, 569, si esprime a favore di «un contraddittorio "per la prova" e non un contraddittorio "sulla prova"».

[52] L'AI consente di «effettuare delle previsioni in termini probabilistici, basate su un'elaborazione statistica di dati e parametri». V. *supra*, 562. Sul tema v., *ex multis*, RICCIO, *Ragionando su intelligenza artificiale e processo penale*, in *questa Rivista*, 2019,3; PIANA, *Dal rito al calcolo e ritorno. Affresco sull'incontro fra il sistema giustizia e l'intelligenza artificiale*, in *questa Rivista*, 2020, 1; POLIDORO, *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*, in *questa Rivista*, 2020, 3; CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, in *Sist. Pen.,* 2021; PAULESU, *Intelligenza artificiale e giustizia penale Una lettura attraverso i principi*, in *questa Rivista*, 2022, 1; MORGANTE - FIORINELLI, *Promesse e rischi della compliance penale digitalizzata*, in *questa Rivista*, 2022, 2; AMISANO, *Prevedere -e non predire- attraverso gli algoritmi e le loro insidie*, in *questa Rivista*, 2022, 2; FLICK, *25 anni di privacy in Italia. Dalla distanza di cortesia all'algoritmo***,** in *Cass. Pen.*, 2022, 7-8; GUIDO, *Intelligenza artificiale e procedimento penale: ragionando di valutazione del rischio de libertate*, in *questa Rivista*, 2023, 1; DE SIMONE, *Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale*, in *questa Rivista*, 2023, 2;

[53] MAGLIULO, *op. cit.*, 562.

Basti pensare all'impiego del software di riconoscimento facciale[54], già utilizzato dal 2017 dalla Polizia di Stato per la sorveglianza a fini di sicurezza e per il supporto all'attività investigativa; mediante la tecnologia del "*Remote biometric identification systems*" (di cui il *software* di riconoscimento facciale costituisce esempio) è possibile scansionare in tempo reale i dati biometrici delle persone presenti in luoghi, anche affollati, al fine di risalire ai singoli individui[55].

Eppure, sebbene in Italia sia stata completata la digitalizzazione del processo civile ed amministrativo, ad oggi non si rinviene una normativa di riferimento per l'intelligenza artificiale, nonostante non manchino tentativi in tal senso; nell'incertezza taluno ha opinato che anche la prova algoritmica dovrebbe ricadere nel paradigma dell'art. 189 c.p.p., ma, come per la prova digitale, si pongono all'interprete i medesimi dubbi interpretativi[56].

La stasi normativa impedisce un inquadramento generale e costringe l'interprete ad un'opera di valutazione casistica, verificando «se lo strumento probatorio relativo al dato digitale utilizzato sia estraneo o meno – e, se sì, sotto quale profilo: fonte di convincimento del tutto nuova oppure diverse

---

[54] DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 2022, 3, 1065-1066, sottolinea come non vada sottostimato quell'eterogeno movimento di pensiero teso a rallentare l'avanzata delle "tecnologie del controllo" in ambito penale, di cui un fulgido esempio è rappresentato dall'intervento di diverse istituzioni europee che, pur non ritenendo necessario spingersi al punto da limitare del tutto l'utilizzo di strumenti di identificazione biometrica, in generale, e al *facial recognition,* tuttavia, hanno caldeggiato l'adozione di cautele minime ad hoc contro il pericolo di una lesione dei diritti fondamentali dell'individuo

[55] MAGLIULO, *op cit.,* 564. Per l'utilizzo del R.B.I.S. è necessario rispettare una serie di garanzie: in primo luogo, è necessaria un'autorizzazione preventiva rilasciata da un organo giurisdizionale o da un'Authority; solo qualora si versi in un caso di urgenza si potrà procedere senza autorizzazione che, tuttavia, dovrà pervenire durante l'utilizzo o al termine per ritenere legittimi i risultati.

[56] SACCOMANI, *op. cit.*, 639, sottolinea come l'ingresso della prova algoritmica nel processo penale sia fonte di possibile violazione del *fair trial* giacché le prove e gli elementi idonei ad incidere sulla determinazione della pena, generati da software o sistemi computazionali, non permettono alla difesa di verificare la genuinità del dato e ciò si riflette sulle garanzie dell'imputato.

MAGLIULO, *op. cit.*, 571, sottolinea come la sensibilità per la tematica sia stata espressa attraverso l'adozione della Carta etica europea per l'uso dei sistemi di intelligenza artificiale nei sistemi di giustizia (2018) da parte della Commissione Europea per l'efficienza della giustizia; quest'ultima fissa i principi generali e le misure utili a favorire l'interazione tra giustizia e tecnologia nei vari ordinamenti. Sul tema anche DEL NINNO, *La proposta di Regolamento UE sull'Intelligenza Artificiale: i profili operativi del nuovo quadro normativo europeo – Parte Prima*, in *Dir. giust.*, 2021; QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Leg. pen.*, 2019.

modalità operative di mezzo già noto – al catalogo legale; e ciò, soprattutto, con riferimento ai mezzi di ricerca della prova digitale»[57].

3. *"L'era digitale" della prova documentale.* Uno dei profili più delicati concerne proprio l'acquisizione al processo di messaggi inviati mediante *whatsapp* (o attraverso altre *chat online*, come *Facebook Messenger)* ed sms[58] attraverso riproduzione fotografica.

La questione si è posta in considerazione della frequenza con cui si ricorre alle applicazioni di messaggistica nella vita quotidiana, che consentono di scambiare messaggi di testo, immagini, documenti, video e anche note vocali; ed è evidente che molte delle informazioni che transitano su dispositivi digitali possono avere una qualche rilevanza anche ai fini processuali. Da qui le difficoltà di inquadramento del fenomeno, che assume diverse connotazioni a seconda della tipologia di informazione, della qualifica del soggetto e delle modalità di apprensione del dato[59].

La giurisprudenza di legittimità, con andamento costante, ha ribadito che «in tema di mezzi di prova, i messaggi *whatsapp* e gli sms conservati nella memoria di un telefono cellulare hanno natura di documenti ai sensi dell'art. 234 cod. proc. pen., sicché è legittima la loro acquisizione mediante mera riproduzione fotografica, non trovando applicazione né la disciplina delle intercettazioni, né quella relativa all'acquisizione di corrispondenza di cui all'art. 254 cod. proc. pen.»[60]. La natura di prova documentale[61] deriva dall'impossibilità,

[57] PITTIRUTI, op. cit., 21.

[58] Anche in ambito civile si discorre di acquisizione di SMS, riconducibili nell'ambito dell'articolo 2712 c.c., con la conseguenza che formano piena prova dei fatti e delle cose rappresentate se colui contro il quale vengono prodotti non ne contesti la conformità ai fatti o alle cose medesime. Tuttavia, l'eventuale disconoscimento di tale conformità non ha gli stessi effetti di quello della scrittura privata previsto dall'articolo 215 c.p.c., comma 2, poiché, mentre, nel secondo caso, in mancanza di richiesta di verificazione e di esito positivo della stessa, la scrittura non può essere utilizzata, nel primo non può escludersi che il giudice possa accertare la rispondenza all'originale anche attraverso altri mezzi di prova, comprese le presunzioni. Cass. Civ., Sez. I, 17 luglio 2019, n. 19155.

[59] In tal senso DEL COCO, *L'utilizzo probatorio dei dati whatsapp tra lacune normative e avanguardie giurisprudenziali*, in *Proc. pen. giust.*, 2018, 3, 107.

[60] Cass., Sez. VI, 08 giugno 2022, Rv. 283319. In senso conforme v. Cass. 1822 del 2020, Rv. 278124; Cass., n. 1822 del 2018, Rv. 272319.

[61] *Ex multis*, in tema di prova documentale, si veda GREVI - ILLUMINATI, *Prove*, in *Compendio di procedura penale*, a cura di Conso – Grevi - Bargis, 2020, 300 ss.; DOMINIONI, *Il diritto delle prove*, in

ravvisata dalla Corte[62], di ricondurre l'ablazione dei dati informatici contenuti nella memoria del telefono all'ambito operativo della captazione, poiché l'attività di intercettazione presuppone un flusso di comunicazioni in atto, diversamente dall'ipotesi di specie ove il dato viene acquisito *ex post*; inoltre, anche la disciplina del sequestro di corrispondenza privata viene esclusa sulla base del fatto che i messaggi *whatsapp* (*et similia*) che vengono appresi dalla memoria del dispositivo non possono rientrare nel concetto di «corrispondenza» di cui al 254[63] c.p.p., in quanto è richiesta «un'attività materiale di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito»[64].

All'evidenza, il punto di svolta è costituito dalla memorizzazione del dato[65], che attesta la sussistenza del fatto storico[66]. Ciò vale non solo per le ipotesi di

---

Procedura penale, a cura AA.VV., Torino, 2023, 355 ss.; VERGINE, *sub art. 234*, in *Comm. c.p.p. online*, a cura di Gaito - AA. VV., 2023; CALAMANDREI, *La prova documentale*, Padova, 1995; ID., *sub art. 234*, in *Comm. c.p.p.*, a cura di Giarda - Spangher, Milano, 1997; CAMINITI, *Prova documentale e giusto processo*, in *Dal principio del giusto processo alla celebrazione di un processo giusto*, a cura di Cerquetti - Fiorio, Padova, 2002, 227; CANDIAN, *Documentazione e documento, teoria generale*, in *Enc. dir.,* XIII, Milano, 1964, 579; CANTONE, *La prova documentale*, Milano, 2004.

[62] Si trattava di una fattispecie relativa a dati - allegati in copia cartacea o trasfusi nelle informative di polizia giudiziaria - acquisiti in separato procedimento, in cui la Corte ha precisato che non è indispensabile, ai fini della loro autonoma valutabilità, l'acquisizione della copia forense effettuata nel procedimento di provenienza, né dell'atto autorizzativo dell'eventuale perquisizione.

[63] Va però precisato che non sono mancati orientamenti di segno diverso (seppur risalenti) che hanno ricondotto gli SMS nella nozione di corrispondenza *ex* art. 254, comma 2 c.p.p. e 353 c.p.p. sulla scorta di una sua lettura estensiva, così secondo RENZETTI, *Acquisizione dei dati segnalati sul display: il rischio di una violazione dell'art. 15 Cost.*, in *Cass. Pen.*, 2006, 2, 542. Intendendosi con corrispondenza ogni «forma attuale di telecomunicazione che assuma la forma scritta al momento della richiesta di spedizione o di ricezione (telegrammi, cablogrammi, telescritti)». Cit. di DE GENNARO- BRUNO, *Polizia giudiziaria e intercettazione di comunicazioni*, in *questa Rivista.*, 1965, 1, 157.

[64] Così secondo NOCERA, *L'acquisizione delle chat whatsapp e messenger: intercettazione, perquisizione o sequestro?*, in *Il penalista*, 2018.

[65] Secondo Cass., Sez. II, 01 luglio 2022, n. 39529, in *www.dejure.it*, che ha ritenuto legittima l'acquisizione mediante mera riproduzione fotografica dei messaggi whatsapp e degli sms conservati nella memoria del telefono, vi sono due profili da sottolineare. In primo luogo, «il testo di un messaggio fotografato dalla PG sul display del dispositivo ha natura di documento, la cui corrispondenza all'originale è asseverata dalla qualifica dell'agente che effettua la riproduzione; inoltre, l'utilizzabilità del contenuto dei messaggi *WhatsApp* scaricati sul PC della persona offesa, è strettamente derivante e conseguente dall'attendibilità delle dichiarazioni accusatorie rese dalla persona offesa. Consegue che ai fini probatori, nell'ambito del procedimento penale, non è necessario estrarre i messaggi *WhatsApp* mediante la procedura della cd. copia forense, essendo sufficiente che la persona offesa faccia fotografare da un agente di PG il messaggio WhatsApp dal display del cellulare oppure scarichi sul proprio PC i messaggi *WhatsApp* ricevuti».

registrazioni di conversazioni tramite *chat* (o telematiche) che abbiano la forma di testo[67], ma anche per le note vocali in cui la conversazione avviene in forma orale, ma con un inizio e una fine ben precisa (venendo poi inoltrata nella medesima *chat*), risultando, quindi, equipollenti al testo scritto dal punto di vista probatorio.

Sarebbe proprio la lettera dell'articolo 234, comma 1, c.p.p. a confermare la tesi secondo cui «è consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo»[68].

Se il dato digitale è rappresentato dal contenuto dei messaggi intercorsi nella chat, il supporto cartaceo che contiene la trascrizione delle conversazioni «si atteggia come una sorta di "prova documentale di secondo livello", legata da un rapporto di "rappresentatività indiretta", "al quadrato" rispetto al contenuto della conversazione che è, a sua volta, incorporato all'interno della memoria del telefono»[69].

Un ulteriore argomento normativo si rinviene nell'articolo 237 c.p.p., che consente sempre l'acquisizione di documenti provenienti dall'imputato.

---

[66] Nello stesso senso si veda Cass., Sez. II, 30 novembre 2016, n. 50986, Rv. 268730, ove la Corte ha osservato che «la registrazione fonografica di una conversazione telefonica effettuata da uno dei partecipi al colloquio costituisce una forma di memorizzazione fonica di un fatto storico, utilizzabile in dibattimento quale prova documentale, rispetto alla quale la trascrizione rappresenta una mera trasposizione del contenuto del supporto magnetico contenente la registrazione. (In motivazione, la Corte ha precisato che la registrazione della conversazione tra presenti è qualificabile quale prova documentale anche nell'ipotesi in cui sia stata effettuata su suggerimento o incarico della polizia giudiziaria)». In senso conforme Cass., Sez. I, 6 aprile 2009, n. 14829, Rv. 243741; Cass., Sez. VI, 22 aprile 2009, n. 16986, Rv. 243256; Cass., Sez. VI, 5 agosto 2011, n. 31342, Rv. 250534; Cass. Sez. I, 8 febbraio 2013, n. 6339, Rv. 254814. In senso difforme v. Cass., Sez., VI, 21 giugno 2010, n. 23742, Rv. 247384; Cass., Sez. II, 13 febbraio 2014, n. 7035, Rv. 258551; Cass., II Sez., 8 maggio 2015, n. 19158, Rv. 263526.

[67] Cfr. NOCERA, *op. cit.*

[68] A parere di alcuni l'operatività dell'articolo 234 prescinde totalmente dal tipo di mezzo utilizzato, potendo agevolmente ricomprendersi il dato digitale. Ad esempio, ROTA, *I documenti*, in *La prova nel processo civile*, a cura di Taruffo, Milano, 2012, 729. PITTIRUTI, *op. cit.*, 23.

[69] DEL COCO, *op. cit.*, 535. L'espressione, a sua volta, è di ROTA, *op. cit.,* 730.

Al riguardo si segnala una pronuncia della Corte di Cassazione che ha ritenuto legittima l'acquisizione da parte del giudice di merito di messaggi inviati attraverso i *social networks Whatsapp* e *Facebook* dall'imputato ad una minore, e da questa messi a disposizione della polizia giudiziaria al momento della presentazione della querela. In tale caso la Corte ha puntualizzato che «per documento proveniente dall'imputato si intende, ai sensi dell'art. 237 cod. proc. pen., il documento del quale è autore l'imputato ovvero quello che riguarda specificamente la sua persona, ancorché da lui non sottoscritto, anche se sequestrato presso altri o da altri prodotto». Cass., Sez. III, 03 agosto 2017, n. 38681, Rv. 270950. In senso conforme Cass., Sez. V, 28 luglio 2015, n. 33243, Rv. 264973.

L'indagine verte anche sulla perimetrazione della nozione di «documento informatico»[70] dovendosi distinguere tra l'inscindibilità del dato dal documento – senza il quale non può essere rappresentato – e la categoria più recente di "tipo digitale", ove vi è piena indipendenza dal supporto; a tracciare una netta differenza è la caratteristica di immaterialità del dato digitale, a cui si può accedere anche in contenitori diversi rispetto a quello dove è stato prodotto. Proprio per tale ragione, il rischio si annida nel «trasferimento», sicché è indispensabile una maggiore cautela per tutelare la genuinità[71] del dato digitale: l'ipotesi di alterazione o compromissione è tutt'altro che peregrina.
Viene da chiedersi, quindi, quanto sia legittimo ricondurre al modello di prova documentale quei dati digitali incorporati in supporti cartacei di cui non è sempre possibile accertare l'autenticità. Basti solo pensare all'ipotesi di *screenshots* estratti dalla *chat* o dai *social networks*[72] che confluiscono nel fascicolo dibattimentale mediante stampa del *file*.
Accade non di rado che il soggetto direttamente coinvolto provveda ad effettuare modifiche, cancellando il *post* originariamente pubblicato o i messaggi inoltrati via *whatsapp*, sicché l'interprete è posto di fronte alla scelta tra negare l'accesso a tale materiale o far fede alla stampa, con tutto ciò che ne consegue in termini di utilizzo probatorio.
Nel primo caso, si rischia di contravvenire al principio di non dispersione della prova e, nell'altro, di acconsentire all'ingresso di elementi potenzialmente inquinati che inficiano la correttezza della verifica giudiziale[73].

---

[70] Si veda in argomento DI PAOLO, op. cit., 739 ss.
[71] DEL COCO, *op. cit.,* 537.
[72] Si veda ad esempio Cass., Sez. V, 30 marzo 2021, n. 12062, Rv. 280758, ove si è precisato che «è legittima l'acquisizione come documento di una pagina di un "*social network*" mediante la realizzazione di una fotografia istantanea dello schermo ("*screenshot*") di un dispositivo elettronico sul quale la stessa è visibile».
[73] La tematica è ricostruita da PITTIRUTI, *op. cit.*, 25. ss. Peraltro, appare oltremodo interessante l'argomento normativo adoperato secondo cui l'articolo 234 *bis* c.p.p. (introdotto nell'ambito della lotta al terrorismo di matrice internazionale), che stabilisce che è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso in tal caso del legittimo titolare, assumerebbe valore di conferma dell'*intentio legis* di equiparare i dati informatici alla prova digitale vista la sua collocazione. Diversamente, potrebbe ritenersi che la scelta lessicale dell'art. 234 *bis* smentisca la corrispondenza del dato informatico con il documento digitale proprio in virtù della considerazione per cui i dati informatici sono differenziati dai documenti nella formulazione della norma, quasi a suggerirne la diversa natura. In argomento v. anche DEL COCO, *op. cit.*, 537.

L'orientamento prevalente riconduce l'acquisizione della *digital evidence* alla prova documentale contenente la rappresentazione di dati digitali, facendo leva sul libero convincimento del giudice[74]. Il che significa che è rimesso alla parte l'onere della prova sull'alterazione del dato[75]. Sono, invece, apprezzabili i tentativi di segno opposto da parte di quella giurisprudenza di legittimità[76], che invita ad un maggiore rigore selettivo, alla luce di una diversa impostazione metodologica, fondata non sul libero convincimento, ma sulle possibili sanzioni conseguenti alla mancata adozione delle cautele idonee ad assicurare la corrispondenza tra il supporto cartaceo e il dato[77].
L'impressione è che il formante giurisprudenziale prevalente avalli suddetta ricostruzione, giustificando anche forzature normative, pur di conservare elementi ritenuti indispensabili, e, quindi, non disperdibili ai fini dell'accertamento del fatto di reato. Ancora una volta il vizio è a monte: l'assenza di un'espressa previsione legislativa, volta a sgombrare il campo da incongruenze sistemiche, favorisce un'interpretazione, a tratti creativa, per la risoluzione delle fattispecie dedotte in giudizio.

---

[74] In argomento, è interessante operare il raffronto con la prova civile e, in particolare, con la riproduzione cartacea delle risultanze di un sito internet. La Cassazione ha precisato che in tema di prova civile, la conformità della riproduzione cartacea delle risultanze di un sito internet può essere oggetto di contestazione ai sensi dell'art. 2712 c.c. e delle norme del codice dell'amministrazione digitale, ma al giudice è sempre consentito - anche d'ufficio ai sensi dell'art. 447 *bis*, comma 3, c.p.c., se applicabile - l'accertamento della contestata conformità con qualunque mezzo di prova, inclusa la richiesta di informazioni al gestore del servizio ai sensi dell'art. 213 c.p.c. ovvero, come nella specie, mediante verifica diretta del sito. (Nella specie, la S.C. ha confermato la correttezza della verifica, svolta d'ufficio dal giudice ed eseguita mediante l'accesso diretto al sito internet del servizio postale degli Emirati Arabi Uniti, dell'esito dell'invio di una raccomandata semplice, trasmessa per la disdetta di un contratto di comodato). Cass. Civ., Sez. III, 26 agosto 2020, n. 17810, Rv. 658689. In tema di efficacia probatoria delle e-mail e degli sms si veda GALLUZZO, *Sms e-mail: piena prova in sede giudiziale*, in *Il Familiarista*, 2019, 11.
[75] DEL COCO, *op. cit.,* 537. Peraltro, l'Autrice sottolinea «che in altri settori, come quello civilistico, inizia a diffondersi una nuova sensibilità nei confronti delle garanzie di autenticità del documento informatico».
[76] Da ultimo il riferimento è a Cass., Sez. V, 24 gennaio 2022, n. 2658, Rv. 282771, che ha precisato che «ai fini dell'utilizzabilità della trascrizione delle conversazioni via "*whatsapp*" effettuata dalla persona offesa, la necessità di acquisire il supporto telematico o figurativo contenente la relativa registrazione deve essere valutata in concreto, tenendo conto della credibilità della persona offesa e dell'attendibilità delle sue dichiarazioni accusatorie». (Fattispecie in tema di atti persecutori, in cui la Corte ha affermato che correttamente il giudice di merito aveva ritenuto superflua la richiesta difensiva di accertamento tecnico e di estrazione dei dati del traffico telefonico delle utenze interessate, non essendovi ragione di dubitare dell'attendibilità delle dichiarazioni della persona offesa in merito alla provenienza e al contenuto dei messaggi). Nello stesso senso v. Cass. Sez. V, 25 ottobre 2017, n. 49016, Rv. 271856.
[77] DEL COCO, *op. cit.,* 538; in argomento v. anche GIUNCHEDI, *op. cit.*, 821 ss.

Un ultimo cenno merita l'acquisizione dei contenuti e-mail che, intesa come "biglietto elettronico", ha natura documentale[78]; va tuttavia segnalato che «il flusso di dati codificati da elaboratori elettronici e, in seguito, trasmessi secondo le più evolute modalità si trasferisce da una fonte di prova a un'altra, rinnovando gli elementi esterni della comunicazione e arricchendo il documento originariamente trasmesso, senza – tuttavia – perdere alcuna delle proprie caratteristiche»[79]. La *querelle* si è innestata su due filoni: da un lato, si è ritenuta applicabile la disciplina di cui all'art. 266 *bis* c.p.p. (con garanzie più rigorose); dall'altro, invece, si è suggerito di procedere all'apprensione mediante sequestro[80], secondo l'art. 254 *bis*, presso il gestore del servizio[81].

---

[78] Un interessante spunto di riflessione è offerto in ambito civilistico, ove la Cassazione ha ritenuto che in tema di efficacia probatoria dei documenti informatici, il messaggio di posta elettronica (cd. e-mail) privo di firma elettronica non ha l'efficacia della scrittura privata prevista dall'art. 2702 c.c. quanto alla riferibilità al suo autore apparente, attribuita dall'art. 21 del d.lgs. n. 82 del 2005 solo al documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, sicché esso è liberamente valutabile dal giudice, ai sensi dell'art. 20 del medesimo decreto, in ordine all'idoneità a soddisfare il requisito della forma scritta, in relazione alle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità. Cass., Sez. L., 08 marzo 2018, n. 5523, Rv. 647611.

[79] Così MANCUSO, *op. cit.*, 501. L'autore precisa inoltre che ogni e-mail consegnata dal server alla casella di posta è da considerarsi documento elettronico autonomo consultabile in rete attraverso un accesso remoto (web access), «"scaricato" sul proprio elaboratore elettronico mediante programmi client di posta, i quali possono essere configurati per cancellare contestualmente o meno il contenuto presente nel luogo virtuale della casella elettronica, ovvero archiviato presso una memoria di cui si ha la disponibilità fisica (hard disk o supporto analogo) o virtuale (archiviazione on the cloud)». Si veda anche ZACCHÉ, *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.*, 2013, 4, 106; ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, 134; CERQUA, *Ancora dubbi e incertezze sull'acquisizione della corrispondenza elettronica*, in *Dir. pen. cont.*, 2015.

[80] L'oggetto del sequestro informatico si sostanzia nei dati, nelle informazioni e nei programmi conservati in ambiente digitale. Altresì, si estende ai contenuti delle e-mail che, in effetti, rappresentano elementi probatori particolarmente utili nelle indagini informatiche. Il sequestro si colloca solitamente a valle di un'attività di ricerca della prova digitale (ispezione o perquisizione) potendo ricadere su oggetti di corrispondenza estranei ai flussi di comunicazione; perciò, esclusi dal perimetro operativo delle intercettazioni di cui all'art. 266 *bis* c.p.p. Così, MANCUSO, *op. cit.*, 529.

[81] MANCUSO, *op. cit.*, 515; Per approfondimenti in tema di sequestro di dati informatici si veda TESTAGUZZA, *Il sequestro di dati e sistemi*, in *Cybercrime,* a cura di Cadoppi – Canestrari – Manna - Papa, Torino, 2019; MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. Pen.*, 2012, 2; MONTI, *La nuova disciplina del sequestro informatico,* in *Sistema penale e criminalità informatica,* a cura di Luparia, 2019; VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, in *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale,* a cura di Luparia, Milano, 2012, 110 ss. Più di recente, CASCONE, *La disponibilità esclusiva del dato informatico: una nuova pronuncia della Corte di Cassazione a tutela "del patrimonio informativo*", in *Cass. Pen.,* 2023, 2.

Se le modalità e l'oggetto del sequestro ne attestano la «natura» statica, legittimandone il ricorso nei casi in cui venga meno la contestualità di trasmissione[82], la captazione dei flussi informatici, in tempo reale, va ricondotta alle regole operative delle intercettazioni.

Invero – come è stato accuratamente notato[83] – il *punctum dolens* si ravvisa nell'ipotesi in cui l'*e-mail* vada acquisita prima che il procedimento comunicativo sia compiuto. Si ripropone la distinzione tra sequestro e intercettazioni: taluni suggeriscono di far ricorso alla disciplina delle intercettazioni quando debbano essere appresi messaggi non letti o di cui non sia certa la lettura; altri, di contro, puntualizzano che è proprio la lettera dell'art. 254 *bis* c.p.p. a prevedere la possibilità di procedere a sequestro di quella corrispondenza inoltrata in via telematica di cui si presume la mancata conoscenza da parte del destinatario (così come gli altri casi di corrispondenza)[84].

Nell'incertezza interpretativa un dato è certo: il sequestro probatorio non può avere valenza esplorativa. A confermarlo è la Cassazione che ha ribadito che «l'acquisizione indiscriminata di un'intera categoria di beni, nell'ambito della quale procedere successivamente alla selezione delle singole "res" strumentali all'accertamento del reato, è consentita a condizione che il sequestro non assuma una valenza meramente esplorativa[85] [...]»[86]. Sicché le regole operative in tema di sequestro non possono venir meno in nessun caso.

Si segnala che, da ultimo, è stato presentato il d.d.l. S. 690 che prevede l'introduzione dell'articolo 254-*ter* nel codice di rito penale recante norme in materia di sequestro di strumenti elettronici. L'intento è di regolamentare il procedimento di sequestro dei dispositivi elettronici riprendendo in parte la normativa sui tabulati telefonici e quella sulle intercettazioni, trovando un punto di convergenza tra la tutela della *privacy* e la salvaguardia delle indagini. Sul tema v. MARTORANA - ZAKARIA, *Privacy e indagini, presentato un DDL sul sequestro di strumenti elettronici*, in *www.altalex.com*, 2023.

[82] Difatti, si ritiene pacificamente che, una volta letta, la corrispondenza inoltrata per posta elettronica vada assoggettata al sequestro (così come i pieghi cartacei). DI PAOLO, *op cit.,* 757.

[83] DI PAOLO, *op. cit.*, 757 ss.

[84] DI PAOLO, *op. cit.*, 758.

[85] In dottrina si è altresì precisato che la perquisizione informatica non può risolversi in un monitoraggio preventivo a fini esplorativi né il carattere informatico è idoneo a modificare tale natura. Così secondo BONO, *Il divieto di indagini ad explorandum include i mezzi informatici di ricerca della prova*, in *Cass. Pen.*, 2013, 4, 1525. In materia di perquisizioni si v. anche PARLATO, *Perquisizioni on-line*, in *Enc. dir., Annali*, X, Milano, 2017.

[86] In tale fattispecie, la Corte, in relazione al reato di finanziamento illecito ai partiti, ha ritenuto esplorativo e sproporzionato il sequestro indistinto di tutte le mail, personali e della società, riferibile ad un soggetto terzo estraneo al reato, trasmesse e ricevute nei dieci anni precedenti (Cass. Sez. VI, 02 dicembre 2020, n. 34265, Rv. 279949). Peraltro, si è anche osservato che, con riferimento al trattenimento oltre il tempo necessario all'estrazione dei dati pertinenti al reato per cui si procede, in tema di seque-

4. *La captazione in tempo reale e le ricadute sui diritti costituzionalmente garantiti*. Il dibattito si fa ancor più attuale con riferimento alle intercettazioni[87] e allo strumento del captatore informatico[88]: emblema del cambiamento tecnologico nelle modalità di acquisizione degli elementi probatori utilizzabili in giudizio[89].

---

stro probatorio di dispositivi informatici o telematici, l'estrazione di copia integrale dei dati in essi contenuti realizza solo una copia-mezzo, che consente la restituzione del dispositivo, ma non legittima il trattenimento della totalità delle informazioni apprese oltre il tempo necessario a selezionare quelle pertinenti al reato per cui si procede. (In motivazione, la Corte ha precisato che il pubblico ministero è tenuto a predisporre un'adeguata organizzazione per compiere tale selezione nel tempo più breve possibile, soprattutto nel caso in cui i dati siano sequestrati a persone estranee al reato, e provvedere, all'esito, alla restituzione della copia-integrale agli aventi diritto).

[87] In via generale sul tema si veda BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte Europea*, in *Cass. Pen.*, 2016, 5. CAPONE, *Intercettazioni e Costituzione. Problemi vecchi e nuovi*, in *Cass. Pen.* 2017, 3; FILIPPI, *Riforme attuate, riforme fallite e riforme mancate degli ultimi 30 anni. Le intercettazioni,* in *questa Rivista,* 2019, 3; BENE, *"Il re è nudo": anomie disapplicative a proposito del captatore informatico*, in *questa Rivista,* 2019, 3
CIAMPI, *La riforma delle intercettazioni le sue ricadute sulla conclusione delle indagini preliminari*, in *questa Rivista,* 2020, 2; SCALFATI, *Intercettazioni: spirito autoritario, propaganda e norme inutili*, in *questa Rivista*, 2020, 1; GRIFFO, *Il captatore informatico ed i suoi multiformi impieghi: le intrusioni non finiscono mai!*, in *Dir. dif.*, 2020, 3; ALVINO, *Fornante indiziario e intercettazioni nel prisma dei mezzi di ricerca della prova: lo standard probatorio e il rilievo delle cause di inutilizzabilità nella valutazione della gravità indiziaria*, in *questa Rivista*, 2021, 3.

[88] In via generale v. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. giust.*, 2016, 5. Da ultimo, SALERNO, *Libertà di comunicazione e disciplina delle intercettazioni: la dimensione costituzionale dei limiti di ammissibilità*, in *questa Rivista*, 2023, 2, che riassume i termini del dibattito giurisprudenziale sull'utilizzazione dei risultati delle intercettazioni in altri procedimenti (art. 270 c.p.p.).

[89] Così per NOCERINO, *Il captatore informatico: un giano bifronte, prassi operative vs risvolti giuridici*, in *Cass. Pen.*, 2020, 2, 1; SCACCIANOCE, *Approvvigionamento di flussi e dati tramite il dispositivo telefonico altrui*, in *Le indagini atipiche*, a cura di Scalfati, 2019, 102-103, precisa che le informazioni reperibili da un dispositivo mobile possono trovarsi sulla carta SIM, sulla memoria rimovibile, o ancora sulla memoria interna del telefono. Dalla SIM possono estrarsi informazioni riguardanti l'utente, (come la *International Mobile Subscriber* Identità), nonché le preferenze di lingua e di rete, la rubrica, i messaggi SMS inviati e ricevuti e gli ultimi numeri chiamati. Dalla memoria interna si ricavano informazioni quali le impostazioni del telefono, il calendario, gli SMS o MMS, il registro delle chiamate, la data e l'ora, le suonerie, i dati necessari per produrre funzioni extra, quali registrazioni audio, video e immagini, i dati generici conservati nella memoria del telefono e le applicazioni eseguibili. Se ne deduce che «[..]i telefoni cellulari siano veri e propri contenitori di una pluralità di informazioni personali, potendo arrivare a contenere, a seconda dei gigabyte di memoria di cui sono dotati, dati equivalenti a milioni di pagine di

Si aprono così nuove frontiere per il giurista[90], costretto a fare i conti con "l'inafferrabile" (*rectius*: l'immateriale), e nuove sfide per l'attività investigativa *lato sensu* intesa[91].

L'indagine si complica con riferimento all'elemento temporale: la disciplina delle intercettazioni – in particolare quelle telematiche[92] (art. 266 *bis* c.p.p.)[93] – riguarda strettamente la fase di ricerca della *digital evidence*[94], ma con riferimento a flussi di dati in transito tra più sistemi informatici o telematici[95]. Al

testo, migliaia di immagini e centinaia di video. È quindi possibile, da parte degli investigatori, ricostruire la vita di una persona utilizzando il telefono cellulare come fonte di prova per il reperimento dello storico delle chiamate, dei contatti, dei messaggi di testo e di quelli multimediali, nonché di foto, video e quant'altro».

[90] NOCERINO, *op. cit.*, 3.

[91] Non a caso il carattere "ubiquo" della prova digitale comporta che la stessa possa essere contenuta ovunque. DI PAOLO, *op. cit.,* 756.

[92] Non è di poco momento che la norma sia stata introdotta con il pacchetto di misure introdotte dalla legge 547/1993 per contrastare la criminalità informatica. DI PAOLO, *op. cit.*, 743.

[93]Il punto di partenza dell'indagine sistematica dev'essere proprio il raffronto tra la disciplina sancita nella lettera dell'art. 266 e del 266 *bis* c.p.p. Se, da un lato, si è sostenuto che l'ambito operativo delle captazioni telematiche sia più esteso delle intercettazioni di conversazioni o comunicazioni – potendo essere disposte oltre che nei casi di cui al 266 c.p.p., anche per qualsiasi reato posto in essere mediante l'utilizzo di strumentazione informatica o telematica – (LUPARIA, *La disciplina processuale e le garanzie difensive*, in *Investigazione penale e tecnologia informatica*, a cura di Lupária - Ziccardi, Milano, 2007, 163; PITTIRUTI, *op. cit.*, 59); non si è fatta attendere l'opinione contraria di chi ha richiamato l'attenzione ad una lettura restrittiva, che sovrapponga i confini operativi delle due norme (FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, 82; PITTIRUTI, *op. cit.*, 59). Orbene, gli argomenti normativi, (primo fra tutti la formulazione dell'art. 266 *bis* che, in maniera aperta richiama senza distinzioni particolari i reati commessi mediante l'impiego di tecnologie informatiche o telematiche, a cui si associa la presenza nell'ordinamento di ipotesi in cui si riconosce l'operatività di un determinato mezzo di ricerca della prova qualora l'offesa sia commessa mediante particolari strumenti, come l'art. 266 co. 1, lett. f) c.p.p.) depongono per una differente interpretazione delle disposizioni *de quibus*, in uno con la *ratio* di destinare tale peculiare mezzo di ricerca della prova all'accertamento di reati realizzati mediante l'utilizzo di tecnologie avanzate per cui sono richiesti strumenti altrettanto innovativi e "tecnicamente" in grado di stare al passo.

[94] In ciò si avverte la necessità di una differenziazione per la *species* delle intercettazioni comunque riconducibile al *genus* dei mezzi di ricerca della prova digitale (altresì contenente ispezioni, perquisizioni e sequestri).

[95] PITTIRUTI, *op. cit.*, 57. Cfr. anche DI PAOLO, *op.cit.*

Si segnala, peraltro, una recentissima pronuncia della Cass., Sez. I, 13 ottobre 2022, n. 6363, che ha precisato che in tema di intercettazioni della messaggistica scambiata con sistema cifrato *Sky Ecc* e *Encrochat*, la decriptazione delle conversazioni e delle comunicazioni è attività distinta dalla captazione, tale che il dato informatico in chiaro, ottenuto dalla trasformazione delle "stringhe" in contenuti intellegibili tramite l'apposito algoritmo messo a disposizione dalla società titolare del sistema operativo, è acquisibile a sensi dell'art. 234-*bis* c.p.p. In tale fattispecie si è osservato che l'attività di acquisizione e di decifrazione di tali dati comunicativi non rientra nel novero delle attività di intercettazione poiché queste ultime postulano la captazione di un flusso di comunicazioni in atto, di tal che non è applicabile la

captatore si riconosce natura onnivora, giacché è in grado «di interpretare qualsiasi funzione investigativa: può fare tutto»[96]. Si tratta, in sostanza, di un *malware*[97] (virus) rientrante nella categoria dei «sistemi informatici di controllo da remoto»
(*Remote Control System*), che consente di attivare e controllare il dispositivo-bersaglio a distanza, «da un qualsiasi altro calcolatore, sfruttando un'architettura di tipo client/server»[98]. Il virus s'insinua «nell'apparato oggetto d'indagine e, nel mentre, tramite il client, il monitorante ne acquisisce il pieno controllo»[99].
La polifunzionalità del captatore[100] consente di acquisire non solo flussi di comunicazioni fra sistemi informatici e telematici (*e-mail*, messaggistica ecc.), ma anche di attivare da remoto microfono, telecamera e rilevare la posizione tramite GPS. Inoltre, come *Trojan,* può insidiarsi nella memoria del dispositivo e acquisire tutte le informazioni ivi presenti arrivando persino a registrare anche tutto ciò che viene digitato sulla tastiera (*keylogging*)[101].
L'aspetto più delicato è però la capacità di effettuare delle istantanee dello schermo del bersaglio in tempo reale, riflettendo[102] le attività compiute dall'utente che ha in uso il dispositivo infettato; in tal modo si acquisiscono le informazioni più svariate attraverso *screenshots* calibrati nel tempo dall'operatore che consentono di apprendere tutto ciò che appare sullo schermo[103]. Si tratta di un'attività di ricerca e di captazione di dati digitali effet-

relativa disciplina processuale contenuta negli artt. 266 e ss. c.p.p., la cui estensione alle intercettazioni dei flussi di comunicazioni relativi a sistemi telematici ovvero intercorrenti tra più sistemi telematici è prescritta dall'art. 266-*bis* c.p.p.

[96] APRATI, *Prime riflessioni sull'assetto normativo del captatore informatico*, in *Cass. Pen.*, 2021, 2, 441.

[97] «L'utilizzo di virus informatici per finalità di accertamento appare fenomeno degno di attenzione anche perché ulteriore testimonianza delle difficoltà classificatorie dei mezzi di ricerca della prova digitale». Così PITTIRUTI, *op. cit.*, 22.

[98] Cfr., *infra*.

[99] La definizione è offerta da NOCERINO, *L'acquisizione di dati mediante screenshot tra intercettazione telematica e prova atipica*, in *Camminodiritto*, 2022, 6, 4.

[100] La polifunzionalità del virus è ben inquadrata da TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017, 12 ss.; NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Padova, 2021, 25 ss.

[101] NOCERINO, *op. cit.*, 4.

[102] Cfr. CONTI - TORRE, *op. cit.*, 562 ss.

[103] NOCERINO, *op. cit.*, 5.

tuata in maniera dinamica, avente ad oggetto «il flusso di dati scambiati tra più sistemi informatici o telematici nel suo divenire»[104].
Se l'acquisizione dei dati – potenzialmente rilevanti ai fini dell'accertamento di fatti criminosi – avviene in tempo reale, inclusi gli scambi di messaggi mediante l'utilizzo di *social* o *app* di messaggistica[105], si travalicano, e di molto, i confini posti dal legislatore per la tutela della riservatezza.
L'attività di accertamento non può tramutarsi in un'apprensione indistinta di qualsiasi dato potenzialmente utile ai fini probatori[106]: la raccolta degli elementi di prova dev'essere corredata da idonee garanzie, contestuali, così da porre le basi per una selezione corretta dei dati rilevanti, dell'idoneità del metodo, della qualità del risultato e, soprattutto, delle cautele necessarie per la loro conservazione. Non va tralasciato che anche nella fase iniziale del procedimento è prevista l'applicazione dei principi di rango costituzionale del contraddittorio, del diritto di difesa e della parità delle parti[107].
Eppure, proprio la materia delle intercettazioni richiede maggior cautela. Ci si riferisce al monitoraggio occulto dei *social media*, giacché il captatore è in grado di registrare quanto appare sullo schermo del dispositivo infettato: non

[104] DI PAOLO, *op. cit.*, 743.
[105] In argomento si è pronunciata anche la Corte di cassazione ritenendo legittima l'acquisizione di contenuti di attività di messaggistica (nella specie, effettuata con sistema *Blackberry*) mediante intercettazione operata ai sensi dell'art. 266 e ss. cod. proc. pen, poiché le *chat*, anche se non contestuali, costituiscono un flusso di comunicazioni. Cass. Sez. III, 23 dicembre 2015, n. 50452, Rv. 265615.
In dottrina si è precisato che il principio di diritto enunciato dalla Cassazione che sembra ammettere una deroga implicita ad uno dei requisiti ritenuti a lungo irrinunciabili per definire il concetto di intercettazione, quale la contestualità del colloquio, non pare condivisibile giacché il flusso che intercorre fra i sistemi telematici non può ritenersi "non contestuale", proprio per la particolare connotazione. Né tantomeno si può opinare che in assenza di adeguata copertura di rete il messaggio inviato mediante chat non pervenga al destinatario in tempo reale, poiché alle stesse conseguenze si arriva qualora non sia possibile effettuare una chiamata vocale in assenza di linea (non ideona a far venir meno però la contestualità dell'atto comunicativo). In attuazione del principio di non contraddizione si ricava che: «le chat sono flussi, i flussi sono contestuali, le chat sono sempre contestuali sicché il requisito della simultaneità dell'atto, così come per decenni elaborato dalla più attenta dottrina (e confermato poi dalla giurisprudenza), non potrà che rinvenirsi anche a fronte dei nuovi strumenti offerti dalla tecnologia del settore». Così TESTAGUZZA, *Chat Blackberry: il sistema "pin to pin". Nascita di un nuovo paradiso processuale*, in *questa Rivista*, 2016, 1, 2-3. Sul punto si veda anche TROGU, *Come si intercettano le chat pin to pin tra dispositivi Blackberry?*, in *Proc. pen. giust.*, 2016, 3.
[106] Come è stato accuratamente notato, l'irruzione nell'accertamento penale di nuove tecnologie si pone in limine con i paradigmi del giusto processo e della formazione della prova in dibattimento. Il dibattito che involge lo studioso richiama quello sorto in relazione alla «prova scientifica». GIUNCHEDI, *op. cit.*, 822.
[107] SCACCIANOCE, *op. cit.,* 105-106.

solo – come precisato – è possibile attraverso gli *screenshots* memorizzare l'*output* video del dispositivo, ma mediante il *keylogger* anche captare quanto viene digitato sulla tastiera fisica o virtuale del dispositivo (peraltro, tali funzioni possono essere utilizzate anche contestualmente). Mediante *l'online surveillance*[108] si controlla la vita virtuale del soggetto attenzionato, con tutto ciò che ne consegue in termini di intrusività nella sfera personale[109].
Peraltro, la stessa attività intercettiva può differenziarsi: l'intercettazione ambientale[110] o il controllo di un'utenza telefonica[111] è ben altra cosa rispetto all'apprensione in tempo reale di flussi di comunicazioni via *web*.

---

[108] Per una ricostruzione dei termini del dibattito giurisprudenziale in materia di *online surveillance* si veda BALSAMO, *op. cit.*, 2276 ss.

[109] L'*online surveillance* va tenuta distinta dalla *online search*, in quanto la prima consente di captare «il flusso informatico intercorrente tra le periferiche — video, microfono, tastiera, webcam — ed il microprocessore del dispositivo bersaglio, consentendo al centro remoto di controllo di monitorare in tempo reale tutto ciò che viene visualizzato sullo schermo c.d. *screenshot,* digitato sulla tastiera c.d. *keylogger* o pronunciato al microfono. Si tratta di software che, prescindendo dalle autorizzazioni dell'utente, si installano in un sistema scelto come obiettivo e ne acquisiscono qualsiasi informazione»; la seconda, invece, permette di copiare (in via totale o parziale) delle unità di memoria del sistema target. GRIFFO, *op. cit.*, 694. In senso tecnico sull'argomento si veda CONTI - TORRE, *op. cit.,* 560 ss.

[110] La disciplina dell'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivi elettronici portatili (c.d. *trojan*) è stata da ultimo incisa – anche se in minima parte – dal decreto-legge 30.09.2021 n. 132, convertito in l. 23 novembre 2021, n. 178. Si è previsto, infatti, che il decreto autorizzativo del giudice debba indicare (non già le ragioni, ma) le «specifiche ragioni» che rendono necessaria tale modalità intercettiva per lo svolgimento delle indagini (art. 267, co. 1 c.p.p.). *Pubblicata in G.U. la L. 23 novembre n. 178 in tema di tabulati telefonici*, in *Pen. dir. proc.*, 2021.

[111] Sul punto va segnalato che, dopo la pronuncia della Corte di giustizia dell'U.E., Grande Sezione del 2 marzo 2021 (causa C-746/18) nel caso H.K., il Governo è intervenuto a risolvere il dibattito sul regime da applicarsi all'acquisizione dei tabulati telefonici e telematici, con l'art. 1 del decreto-legge 30.09.2021 n. 132, "Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP" 1. Il tema afferisce alla disciplina della '*data retention*', cioè «della conservazione e acquisizione dei dati "esterni" generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica», che da sempre presenta criticità nella ricerca di un equilibrio tra l'accertamento delle fattispecie di reato e il diritto alla riservatezza. Il legislatore domestico si è voluto adeguare parametri da anni imposti dalla legislazione europea e dalla giurisprudenza sovranazionale. Tuttavia, il percorso non può dirsi interamente completato, giacché – come è stato rilevato – andrebbe rivista anche la durata dei termini di conservazione dei tabulati, che incide fortemente sul principio di proporzionalità. Così RINALDINI, *La nuova disciplina del regime di acquisizione dei tabulati telefonici e telematici: scenari e prospettive*, in *Giur. pen. web*, 2021, 10. Sul tema dei tabulati telefonici v. anche, BERTUOL, *La nuova disciplina per l'acquisizione dei tabulati telefonici: l'interpretazione "autentica" del Legislatore e la parola fine alla (fin troppo) lunga querelle giurisprudenziale*, in giur. pen. web, 2021, 12; CIPRANDI, *La Cassazione si pronuncia sull'utilizzabilità nei processi pendenti delle "acquisizioni telefoniche e telematiche" precedenti all'entrata in vigore dell'art. 1 del D.L. 132/2021*, in *Sist. Pen.*, 2022.

Il paradigma legale di cui all'art. 15 Cost., che tutela la libertà e la segretezza della corrispondenza e ogni altra forma di comunicazione, in assenza di compiuta regolamentazione della materia, rischia di rimanere privo di concreta attuazione[112].

Vieppiù che non tutte le attività consentite mediante captatore presentano il medesimo grado di pervasività[113]. Si ripropone con forza la questione dogmatica, fuori da logiche meramente classificatorie: il nodo da sciogliere riguarda proprio l'inquadramento probatorio delle "altre attività" che il virus può dispiegare.

Il dibattito[114] si è assestato su due filoni dottrinali ritenendosi, da un lato, del tutto illecite quelle attività non strettamente sussumibili nella lettera dell'art. 266[115] e, dall'altro, ammesso un utilizzo di quei risultati che siano quantomeno tipici[116].

A fondamento del primo orientamento vi è l'argomento normativo, giacché non è fatta menzione di funzioni diverse dalle modalità di captazione descritte dagli artt. 266 e 266 *bis* c.p.p. L'esclusione categorica garantirebbe a monte la tutela dei diritti fondamentali.

D'altro canto, si potrebbe però opinare che l'assenza di espressa previsione legislativa non consente di ritenere del tutto esclusa l'ammissibilità di nuove modalità d'investigazione. In primo luogo, perché alcune tra queste possono ricondursi alla disciplina delle intercettazioni, ampiamente regolamentata; inoltre, depone in senso del tutto contrario l'assenza del canone della tassatività della prova nel sistema processuale penale, che trova conferma nella previsione dell'art. 189 c.p.p., disciplinante la prova atipica[117].

---

[112] SANNA, *op. cit.*, 4

[113] CONTI- TORRE, *op. cit.*, 563, precisa che si possono monitorare in via occulta i social mediante *screenshot* e *screencast* senza ricorrere allo strumento del *keylogger software*, quantomai invasivo. In tal senso, da un lato si sostiene che il regime di utilizzabilità è condizionato dal tipo di dato visualizzato dall'utente; dall'altro, che ciò che rileva è il grado di invasività dell'attività di captazione, indipendentemente dal dato captato (ciò in linea con una interpretazione più garantista dei diritti fondamentali dell'individuo).

[114] La complessità del dibattito è riproposta nello scritto di NOCERINO, *op. cit.*, 14 ss.

[115] Così ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma,* in *Riv. it. dir. proc. pen.*, 2018, 2, 538 ss.; SIGNORATO, *Le indagini digitali, profili strutturali di una metamorfosi investigativa*, Torino, 2018, 299 ss.

[116] BRONZO, *L'impiego del trojan horse informatico nelle indagini penali*, in. *Riv. it. sc. giur.*, 2017, 8, 347 s.; CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. Bras. de Direito Processual Penal,* 2017, 3(2), 485 ss.

[117] NOCERINO, *op. cit.*, 15

Non può trascurarsi quel filone giurisprudenziale che ha riconosciuto in tema di videoriprese effettuate "da remoto", mediante l'attivazione attraverso il c.d. virus informatico della telecamera di un apparecchio telefonico smartphone, la natura di 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[118].
Il tentativo di riportare alla legalità la congerie di elementi investigativi appresi con le nuove modalità tecnologiche si scontra, tuttavia, con la configurazione propria dello schema della prova atipica, che, da un lato, attribuisce al giudice un potere istruttorio e, dall'altro, prevede che le modalità di assunzione siano definite con la partecipazione delle parti.
Eppure, quando sono in gioco diritti inviolabili difficilmente può giustificarsi l'elasticità di un meccanismo, che si origina dall'assenza di una chiara e precisa opzione legislativa di bilanciamento[119]. Si avverte l'esigenza preponderante di intervenire nuovamente sull'utilizzo del captatore, regolando le attività di *online surveillance*. L'uso atipico del *Trojan* dovrebbe costituire quasi un'*extrema ratio* a cui ricorrere in casi strettamente necessari: per un verso, andrebbero limitate le categorie di reati per cui è possibile disporre un vero e proprio monitoraggio della vita virtuale dell'individuo e, per altro verso, an-

[118] Si tratta di Cass., Sez. VI, 26 giugno 2015, n. 27100, Rv. 265655. Ne deriva che nel caso in cui l'oggetto della videoregistrazione si sostanzi in mere immagini (*rectius*: comportamenti non comunicativi), il dato acquisito vada ricondotto alla disciplina di cui all'art. 189; diversamente, quando sono appresi anche contenuti comunicativi (un dialogo tra due persone a gesti) a venire in gioco sono le intercettazioni ambientali. NOCERINO, *op. cit.*, 18.
Più di recente Cass., Sez. III, 26 novembre 2021, n. 43609, Rv. 282164, ha precisato che «in tema di prove atipiche, sono legittime e, pertanto, utilizzabili, senza che necessiti l'autorizzazione del giudice per le indagini preliminari, le videoriprese dell'ingresso e del piazzale di un'impresa, eseguite dalla polizia giudiziaria a mezzo di impianti installati sull'edificio antistante, non configurandosi, in tal caso, alcuna indebita intrusione nell'altrui domicilio, posto che i luoghi suddetti non rientrano in tale nozione. (Fattispecie di videoriprese aventi ad oggetto la mera presenza di cose o persone e i loro movimenti)». Per una ricostruzione della sentenza si v. LANDOLFI, *Le videoriprese investigative tra gli incerti confini giurisprudenziali e le crescenti esigenze di tutela della privacy*, in *questa Rivista*, 2022, 1.
[119] Così SANNA, *op. cit.*, 5-6, che, peraltro, precisa che già le Sezioni unite Prisco, avevano sottolineato che l'art. 189 richiede in prima battuta la formazione lecita della prova per ritenerla poi ammissibile e che le Sezioni unite Scurato, nella presa di consapevolezza che il silenzio legislativo osta alla circoscrizione delle potenzialità del *trojan* entro limiti compatibili con il dettato costituzionale (art. 14 e 15 Cost.), hanno riconosciuto la sussistenza di un divieto dell'uso del mezzo riguardante l'intera area dei procedimenti ordinari. In conformità al principio di legalità andrebbero quindi ritenuti inammissibili quegli usi non specificamente regolati dal legislatore. In argomento anche CONTI-TORRE, *op. cit.*, 537.

drebbero rafforzate le sanzioni, qualora siano stati travalicati i limiti legali (e violate le garanzie).
Ricorrere al 'contenitore' della prova atipica per ricomprendere attività investigative altamente intrusive risulta la strada più semplice, ma non la più rispettosa in termini di *privacy* dell'individuo[120].
In assenza di una specifica normativa non è appropriato il rinvio alla disciplina predisposta nel 2008[121] per la prova informatica, avendo il telefono cellulare peculiarità proprie. Sicché, l'aver arricchito l'ambito operativo di istituti processuali preesistenti con l'introduzione di nuove regole per l'informatica forense non pone fine al dibattito[122].

5. *Rilievi conclusivi.* Recentemente, con sentenza 7 ottobre 2021, n. 3591[123], la Prima Sezione della Cassazione Penale si è espressa sul tema ritenendo legittime le attività di *online surveillance* effettuate mediante captatore informatico, poiché inquadrabili nell'alveo delle intercettazioni informatiche o telematiche. L'argomento dirimente si fonda proprio sull'acquisizione del file in tempo reale: in assenza di un'attività di ricerca e di estrapolazione del materiale preesistente dal supporto andrebbe esclusa l'ipotesi della perquisizione[124].

---

[120] Dubbi sorgono proprio in considerazione della formulazione della norma che consente l'ingresso alla prova atipica (art. 189 c.p.p.), quantomai generica, né potrebbe essere diversamente se si considera che ha il precipuo scopo di consentire l'accesso ad atti non tipizzati. Ne deriva che l'apertura del sistema può rivelarsi l'insidia più rilevante per le garanzie fondamentali giacché, per com'è configurata, non soddisfa *in toto* la riserva di legge. Si rende necessaria, dunque, una lettura costituzionalmente orientata, volta ad ammettere quelle prove che non entrino in rotta di collisione con beni costituzionalmente tutelati e che perciò non necessitano di una disciplina espressa. In tal senso si assiste ad una chiusura del sistema più che ad un'apertura. Così per CONTI- TORRE, *op. cit.*, 537.
[121] Si vuole intendere la l. 48/2008 di ratifica della Convenzione di Budapest.
[122] SCACCIANOCE, *op. cit.,* 107.
[123] Per una prima analisi della sentenza v. ALGERI, *Lo Screenshot eseguito (senza garanzie?) dal Trojan di Stato. (Captatore informatico),* in *Giur. it.*, 2022, 12; PROCACCINO, *Piccoli equivoci senza importanza: tra intercettazioni di flussi informatici, perquisizioni e prove atipiche*, in *Cass. Pen.*, 2022, 9.
[124] La Corte precisa che «sul punto, il Tribunale del riesame ha rilevato che il *file excel* è stato "fotografato" sul personal computer in uso all'imputato dal malware ivi inoculato: tale attività investigativa non ha riguardato l'estrapolazione dal supporto digitale di documenti informatici preesistenti all'attività intercettiva, bensì esclusivamente la captazione di flussi di dati in fieri, cristallizzati nel momento stesso della loro formazione. Una tale attività di mera "constatazione" dei dati informatici in corso di realizzazione, pur non costituendo una "comunicazione" in senso stretto, costituisce certamente, invece, un comportamento cd. comunicativo, del quale è ammessa la captazione – previo provvedimento autorizzativo dell'A.G. – nonché la videoregistrazione, dunque anche la fotografia, nel caso di specie mediante screen shot della schermata. Pertanto, non è stata ravvisata alcuna perquisizione, essendo mancata qualsiasi ricerca e successiva estrapolazione di materiale preesistente dal supporto informatico, e – deve aggiun-

Il dibattito in materia si dipana in tre filoni consolidati[125].
In primo luogo, in assenza di una definizione puntuale di «intercettazione» si ritiene pacifica quella offerta da Cass. Sez. Un., 25.5.2003, n. 36747, Torcasio, ove quest'ultima viene intesa come la «captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti».[126]
Inoltre, con riferimento alla nozione di «comunicazione», giurisprudenza[127] e dottrina concordano nel conferire rilevanza alla volontarietà dell'atto e alla partecipazione per la sua formazione di una pluralità di soggetti[128].
Infine, l'oggetto delle intercettazioni di comunicazioni telematiche ed informatiche, stando alla previsione legislativa di cui all'art. 266 *bis* c.p.p., è da intendersi come il flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi. La Corte[129], nel ricostruirne i profili paradigmatici, ha sottolineato che in adesione al dettato normativo l'oggetto debba essere di tipo comunicativo. Ne deriva che affinché possa parlarsi di comunicazione è necessario il requisito della partecipazione di più soggetti e di un «comportamento comunicativo».

---

gersi – non rileva che in tale prospetto in fieri figurino dati preesistenti alla sua formazione, ciò risultando necessitato dalla natura del medesimo, riportante poste di contabilità, ex se riepilogative di operazioni economiche già effettuate ovvero in corso di realizzazione, delle quali si aggiorna annotazione e memoria. Come è stato affermato in arresti giurisprudenziali di questa Corte, «sono legittime le intercettazioni di comunicazioni informatiche o telematiche, di cui all'art. 266-*bis* cod. proc. pen., effettuate mediante l'istallazione di un captatore informatico (c.d. "*trojan horse*") all'interno di un computer collocato in un luogo di privata dimora. (Cass., Sez. V, 30 maggio 2017, n. 48370, Occhionero)». Cfr., anche, PROCACCINO, *op. cit.*, 3121.

[125] I termini del dibattito sono ricostruiti da FROVA, *La Cassazione sulla riconducibilità dell'art. 266 c.p.p. degli screenshot tramite captatore informatico*, in *Sist. Pen.*, 2022.

[126] In particolare, si è osservato che la comunicazione debba presentare carattere riservato e che l'ascolto non debba essere inteso in senso "fisiologico", ma effettuato attraverso la predisposizione di strumenti tenici e, inoltre, che il dispositivo consenta la percezione del dialogo, non solo «la registrazione di quanto viene fisiologicamente percepito» CAPRIOLI, *Intercettazioni e tutela della privacy nella cornice costituzionale*, in *Cass. Pen.*, 2021, 4, 1142.

[127] *Ex multis,* Cass. Sez. VI, 10 novembre 1997, n. 4397, Greco.

[128] FROVA, *op. cit.*, 2-3, precisa che in giurisprudenza si ritiene consolidato quell'indirizzo che considera «comportamenti comunicativi» quegli «atti finalizzati a trasmettere il contenuto di un pensiero con la parola, i gesti, le espressioni fisiognomiche o altri atteggiamenti idonei a manifestarlo, mentre sono comportamenti "non comunicativi" [...] tutti quelli, diversi dai primi, che rappresentano la mera presenza di cose o persone ed i loro movimenti, senza alcun nesso funzionale con l'attività di scambio o trasmissione di messaggi tra più soggetti» (Cass., Sez. III, 21 novembre 2019, n. 15206).

[129] Con riguardo al contesto giurisprudenziale si v. Cass., Sez. un., 13 luglio 1998, n. 21; Cass., Sez. IV, 28 giugno 2016, n. 40903, Grassi; Cass., Sez. un., 23 febbraio 2000, n. 6; Cass. Sez. V, 14 ottobre 2009, n. 16556.

La recente pronuncia[130] si pone in contrasto con gli indirizzi precedenti. Il punto di rottura vero e proprio si rinviene nella ridefinizione della nozione di "comportamento comunicativo". Difatti, includendo anche l'attività di mera constatazione dei dati informatici in corso di realizzazione si disconoscono gli orientamenti consolidati. Il *focus* si sposta sulle modalità della percezione più che sulla valutazione dell'oggetto; si supera la tesi secondo cui affinché possa discorrersi di attività intercettiva sia necessaria la finalità di scambio tra più soggetti di messaggi per porre l'attenzione sulla contestualità della realizzazione dei dati informatici da apprendere[131].

La Prima Sezione sembrerebbe dunque aver preso chiara posizione sulla sorte delle attività di *online surveillance*, oggetto di annoso dibattito, ricorrendo al paradigma normativo delle intercettazioni per includere quelle attività investigative di difficile inquadramento.

Tale ricostruzione risolverebbe *in nuce* le problematiche riconnesse all'applicazione dell'art. 189 c.p.p. che, con riferimento alle attività di *online surveillance,* pone diversi interrogativi circa la natura dei diritti coinvolti nelle operazioni[132].

Invero, attingendo alla giurisprudenza è possibile effettuare ulteriori distinzioni. In primo luogo, è verosimile che si configurino prove atipiche che ledono diritti "emergenti", ossia afferenti a quelle situazioni soggettive indotte dalla modernità e che trovano riscontro nella clausola aperta di cui all'art. 2 Cost. (conformemente alla teoria monista). Ancora, possono profilarsi prove atipiche che seppur riconnesse ai diritti fondamentali non ne intaccano la sostanza, ma solo i limiti esterni. Si è opinato che per tali situazioni potrebbe addirittura adottarsi un modello di tutela meno forte della duplice riserva di legge e giurisdizione, giacché non viene inciso il nucleo dei diritti *de quibus*[133].

Il limite per l'applicazione del modello di prova atipica[134] è il principio di non sostituibilità, che implica l'impossibilità di assumere prove non tipizzate che possano ledere i diritti fondamentali dell'individuo tutelati dalla riserva di legge. E, tuttavia, il quadro si complica con l'inserimento dei nuovi mezzi tecnologici. Definire *ab origine* i profili di interconnessione tra l'utilizzo dei dispo-

[130] Cass., Sez. VI, 29 gennaio 2021, n. 3591.
[131] V. *infra.*
[132] FROVA, *op. cit.,* 6.
[133] Così per CONTI- TORRE, *op. cit.*, 538 ss.
[134] Cfr. anche NOCERINO, *op. cit.*

stivi elettronici e la *plateforme* di diritti coinvolti non è impresa agevole[135], peraltro aggravata dalla mancanza di una presa di posizione espressa da parte del legislatore. In tali ipotesi il rischio di un aggiramento delle garanzie diviene elevato, soprattutto perché le ricadute coinvolgono la sfera più intima dell'individuo.

L'adesione al più recente indirizzo, che allarga notevolmente le maglie operative delle intercettazioni, disvela diverse e ulteriori criticità[136].

In primo luogo, appare condivisibile l'indirizzo della giurisprudenza europea[137] secondo cui ogni intromissione rivesta di per sé la caratteristica di ingerenza della pubblica autorità nella sfera privata, anche qualora non ne sia fatto un uso processuale; ciò in considerazione del fatto che la sanzione dell'inutilizzabilità[138] non offre la "soluzione a tutti i mali". Sotto tale profilo l'approccio del legislatore, prettamente focalizzato sull'utilizzo (o non utilizzo) dei dati raccolti, pur in presenza di violazioni dei diritti fondamentali, risulta parziale.

Difatti, il divieto di utilizzo dei dati concerne il contenuto di conversazioni e comunicazioni intercettate mediante il *Trojan*, non facendo riferimento alcuno alle ulteriore attività che da quest'ultimo possono essere dispiegate (giacché non provviste di copertura legislativa). Limitare le conseguenze all'ambito probatorio significa non tener conto del grado di pervasività della raccolta che si realizza mediante strumenti che consentono di apprendere informazioni in via indistinta e indiscriminata. Fa ben sperare una recente pronuncia del Giu-

---

[135] FROVA, *op. cit.,* 6.

[136] Cfr. FROVA, *op. cit.*, 7; TORRE, *L'intercettazione di flussi telematici (art. 266 bis c.p.p.*), in *Cybercrime*, a cura di Cadoppi – Canestrari – Manna - Papa, Milano, 2019, 1465.

[137] Così Corte Edu, Grande Camera, 25 marzo 1998, Kopp c. Svizzera, n. 23224/1994; Sul punto nella nota informativa, con riferimento all'art. 8 della Convenzione, è precisato che «As interception constituted a serious interference with private life and correspondence, it had to be based on a "law" that was particularly precise, especially as the technology available for use was continually becoming more sophisticated».

[138] Volgendo lo sguardo alle sanzioni apprestate dal legislatore nel caso di inutilizzabilità delle informazioni apprese mediante intercettazione illegittima (271 c.p.p.) o nel caso di trasmigrazione del dato captato (270 c.p.p.) si rende necessaria una precisazione. Ebbene, in dottrina e giurisprudenza si discute della potenziale propagazione del vizio dell'atto illegittimo alla prova ulteriore di cui favorisce l'acquisizione. Di fatto, aderendo alla teoria che ritiene non operante il principio di estensione del vizio agli atti consecutivi e dipendenti, il rischio paventato è che i risultati, inutilizzabili a fini probatori, conserverebbero efficacia a fini investigativi; in tal senso il divieto verrebbe aggirato consentendo l'ingresso forzato di materiale non utilizzabile. Così NOCERINO, *op. cit.*, 24.

dice delle leggi[139] in cui s'intravedono possibili spazi per il riconoscimento di regimi di invalidità differenziati a seconda della tipologia dell'attività investigativa. L'*optimum* sarebbe impedire che di quei dati sia fatto un uso in qualsiasi ambito, anche meramente procedimentale[140].
Lo scenario che si presenta all'interprete è quello di «mera giustapposizione di una dimensione fisica predominante ad una dimensione digitale (residuale e mal tollerata)»[141] da cui derivano sperequazioni trattamentali.
Con l'avvento della Riforma Cartabia si sarebbe auspicata una chiara presa di posizione da parte del legislatore, affinché venisse predisposto un *corpus* organico di norme volte a dare compiuta disciplina alla *digital evidence*.
L'inattività del legislatore lascia ancor più perplessi in considerazione della spinta alla digitalizzazione che ha voluto imprimere al processo penale. L'implementazione del processo telematico[142] costituisce uno dei *leitmotiv* della Riforma; le novità concernono la formazione, il deposito, la notificazione e la comunicazione degli atti con lo scopo di incentivare la transizione digitale. Si discorre della creazione di un vero e proprio «ambiente digitale per il procedimento penale» da realizzarsi mediante le modifiche apportate al Libro sugli Atti e a quelli successivi (una su tutti la previsione della videoregistrazione della prova dichiarativa e dell'interrogatorio)[143]. Peraltro, proprio la nuova regolamentazione della prova scientifica – accostabile alla prova digitale per l'alto tasso di tecnicismo – costituiva l'occasione per porre fine al dibattito giurisprudenziale e dottrinario definendo i contorni normativi della *digital evidence*. Per la prima, il legislatore delegato ha previsto una *discovery* preventiva con riferimento agli elaborati dei periti e dei consulenti tecnici di parte per assicurare contraddittorio tra le parti in fase di assunzione della prova scientifica (art. 501 co. 1 *bis* e 1 *ter* c.p.p.). In tal senso il punto focale dell'intervento è rappresentato dalla necessità di garantire un confronto dialettico e si spiega alla luce del fatto che, diversamente dalla prova dichiarativa,

[139] Corte cost., 26 novembre 2020, n. 252
[140] NOCERINO, *op. cit.*, 25-26.
[141] GALGANI, *Digitalizzazione e processo penale*, in *Quest. giust.*, 2021.
[142] Per un approfondimento sulle ragioni sottese allo sviluppo del processo penale telematico con riferimento alla disciplina emergenziale si v. CANANZI, *Dall'emergenza alla legge delega al Govero: verso un processo penale veramente telematico?*, in *Sist. Pen*, 2023, 3. Più in generale, si veda DELVECCHIO, *Prospettive e tempi della digitalizzazione del processo*, in *Proc. pen. giust.*, 2022, 1; GIALUZ, *Per un processo penale più efficiente e giusto. Guida alla lettura della Riforma Cartabia*, in *Sist. Pen.*, 2022, 5 ss.; TRAPELLA, *La rivoluzione digitale alla prova della riforma*, in *questa Rivista*, 2022, 3.
[143] In questo senso Relazione Ufficio del Massimario, 2023, 2, 1.

nel caso di prova tecnico-scientifica il contraddittorio presenta una configurazione più articolata[144]. Trasponendo in sede di prova digitale le medesime considerazioni, dovrebbe trarsi la conclusione che anche in questo caso sia necessario garantire un contraddittorio, soprattutto in considerazione dei diritti che vengono in gioco.

Su diverso versante si pone la modifica dell'oggetto delle richieste di prova destinataria di recente intervento normativo; il legislatore delegato ha infatti previsto che le parti alleghino i profili di ammissibilità per prove di cui domandano l'assunzione, secondo i parametri dell'art. 189 c.p.p. per le prove atipiche. Si vuole in tal senso garantire che venga verificata l'idoneità ad assicurare l'accertamento dei fatti e il mancato pregiudizio della libertà morale della persona. Per le prove tipiche, invece, l'art. 493 c.p.p., co. 1, richiama per le stesse i canoni di legalità, non manifesta superfluità o irrilevanza sanciti dalla lettera dell'art. 190 c.p.p. Dalla relazione illustrativa si evince che lo scopo avuto di mira dal legislatore è evitare «un ingresso incontrollato di prove nel dibattimento», con l'introduzione di un momento di confronto tra le parti con riguardo alle richieste istruttorie che agevoli il sindacato giudiziale[145]. Pur non trattandosi di una modifica innovativa, essa sposta l'attenzione sul rispetto della impermeabilità tra le fasi. Ebbene, se venisse predisposto un apposito modulo probatorio per la prova digitale, unitamente al richiamato rispetto dei requisiti per l'ammissione delle prove in dibattimento si garantirebbe maggior controllo sul risultato finale e sugli elementi oggetto della valutazione del giudicante.

Tuttavia, non può sottovalutarsi il dato temporale: la modernizzazione è inarrestabile e così l'unica certezza è il mutamento costante delle strutture e delle forme, specchio della società. Non è possibile pensare d'imbrigliare il progresso e ciò che oggi risulta all'avanguardia potrebbe essere desueto domani.

Diversamente, se la strada prescelta è la prova atipica[146] non può trascurarsi l'esigenza di un rafforzamento delle garanzie giacché il grado di pervasività

[144] V. *Supra*, 127- 128.

[145] V. *Supra*, 127.

[146] Più di recente Cass. Sez. IV, 07 giugno 2022, n. 21856, Rv. 283386, ha osservato, con una pronuncia *tranchant*, «che la localizzazione "da remoto", a mezzo di sistema di rilevamento satellitare (GPS), degli spostamenti di un soggetto, rientrante fra i mezzi atipici di ricerca della prova, è utilizzabile nel processo penale senza necessità di autorizzazione preventiva da parte dell'autorità giudiziaria, in quanto non si risolve in una interferenza con il diritto alla riservatezza delle comunicazioni, né in una lesione dell'inviolabilità del domicilio. (In motivazione, la Corte ha chiarito che nella specie non trovano applicazione

nella sfera del soggetto è troppo elevato. L'eccessiva discrezionalità rimessa in capo al giudicante si traduce in un *minus* di controllo sulla qualità del materiale; anche nel caso di prova atipica valgono le considerazioni espresse in tema di prova documentale. Per gli *screenshots* su supporto cartaceo il viatico della prova documentale risulta il più idoneo ad assicurare maggiori garanzie, più del paradigma della prova atipica. Nel caso di *online surveillance* l'esigenza è ancor più avvertita giacché si tratta di monitorare la vita virtuale di un individuo, con poche limitazioni. È evidente allora che il ricorso al mezzo di ricerca della prova atipico diviene un vero e proprio *escamotage* accettabile nella misura in cui viene impedita la dispersione di materiale utile ai fini dell'accertamento.

La tenuta del sistema è precaria. Il paradigma della prova atipica, così come impostato, non è sufficiente a neutralizzare i rischi di una compromissione delle garanzie. Pertanto, andrebbe individuato un nuovo modulo atipico digitale a fronte dell'impossibilità di circoscrivere le novità tecnologiche ad una specifica enucleazione (che peraltro sarebbe distonica con il sistema che non è tassativo). Andrebbe prevista una clausola generale e, allo stesso tempo, andrebbero definiti limiti più stringenti per evitare il c.d. pregiudizio alla libertà morale dell'individuo. Inoltre, si potrebbe anticipare il momento dialettico per assicurare un'attiva partecipazione delle parti in merito al tipo e alla qualità del materiale probatorio, riducendo il rischio che nel processo transiti materiale spurio.

In ogni caso, non si può fare a meno di un'apposita sanzione di inutilizzabilità per la *digital evidence* con conseguente distruzione del materiale raccolto da ritenersi non utilizzabile *in toto.*

Se, invece, conformemente al richiamato indirizzo giurisprudenziale, si prediligesse la categoria delle intercettazioni, sarebbe auspicabile l'introduzione di un'apposita disciplina che si occupi di stabilire requisiti stringenti per l'utilizzo del *Trojan* e, in particolare, per i suoi "usi atipici".

Distinguere le tipologie di attività intercettive in considerazione del tipo di dato captato potrebbe assicurare maggiore tutela dei diritti coinvolti e così offrire un apparato maggiormente garantistico al soggetto sottoposto a "sorveglianza continua".

---

le previsioni degli artt. 244 e 247, comma 1-*bis*, cod. proc. pen. non dovendosi assicurare tracce del reato acquisite tramite ispezioni o perquisizioni)».

Vero è che in tale momento storico si assiste ad un particolare fermento per la materia delle intercettazioni. Basti pensare alla riforma delle intercettazioni preventive d'intelligence (introdotte nell'ordinamento italiano nel 2005 come strumento di contrasto al terrorismo internazionale) contenuta nella manovra finanziaria del 2023[147]; ovvero al recente disegno di legge presentato dal Ministro Nordio, il cui dichiarato intento è assicurare maggiore riservatezza, ampliando il divieto di pubblicazione del contenuto delle intercettazioni[148].
L'attualità del dibattito su temi come *privacy*, trattamento dei dati personali[149], segretezza, riservatezza, unitamente alla riconosciuta indispensabilità delle nuove tecnologie e al loro sempre più frequente utilizzo in ambito processuale, consentono di ben sperare in merito al superamento della stasi normativa; se la *digital evidence* e i diritti dell'individuo possono essere letti come un'endiadi, la rinnovata sensibilità per la tutela della sfera personale può costituire il punto di partenza per una sistematizzazione completa della prova digitale, variamente classificata. Inoltre, se per la *digital forensics* si aprono scenari ancor più favorevoli alla luce della recente attenzione legislativa per la prova scientifica, non è peregrina l'ipotesi che il processo di digitalizzazione acceleri giungendo a livelli ben più accettabili (come in ambito civile ed amministrativo).
Lo stato dell'arte ci induce a supporre che la valutazione legislativa si orienterà nel senso di una riperimetrazione della prova documentale con riferimento all'apprensione di dati digitali (plausibilmente sulla falsariga di quanto sta accadendo in materia di sequestro di strumenti elettronici), mentre per la captazione in tempo reale verrà ridefinita la disciplina dell'attività intercettiva; è meno convincente ritenere, di contro, che la scelta possa ri-

[147] Si intendono attività tecniche eseguite prima della commissione del fatto ed assolutamente inutilizzabili nel procedimento penale, dirette «a raccogliere informazioni utili per la prevenzione di gravi reati e non per l'acquisizione di elementi finalizzati all'accertamento della responsabilità per singoli fatti delittuosi». NOCERINO, *La riforma delle intercettazioni preventive d'intelligence*, in *Sist. Pen.*, 2023, 1; CANTONE - D'ANGELO, *Una nuova ipotesi di intercettazione preventiva,* in *Le nuove norme di contrasto al terrorismo*, a cura di Dalia, 2006, 54.
[148] Comunicato stampa del Consiglio dei ministri n. 39, 15 giugno 2023, in *https://www.governo.it/it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-39/22911.*
[149] È innegabile che la riforma del processo penale incida inevitabilmente su tematiche inerenti alla protezione dei dati personali, toccando temi vicini al diritto della *privacy*. Infatti, proprio per tale ragione, è stato richiesto dal Consiglio dei ministri il parere del Garante Privacy alla riforma (come prevista dall'allora schema di decreto legislativo). MARTORANA - ZAKARIA, *Garante Privacy: ok alla riforma del processo penale*, in *www.altalex.com*, 2023.

cadere sul modello di prova atipica. D'altronde, è proprio l'assenza di una specifica regolamentazione che spinge il formante giurisprudenziale a inscrivere nello schema dell'art. 189 c.p.p. materiale probatorio qualitativamente diverso, seppur riconducibile al più ampio *genus* della prova digitale.