MICHELA SIRACUSA

Il Giano bifronte: autorità e libertà nella *data retention*. *A proposito di una recente pronuncia della Cassazione.*

Il progresso informatico ha permesso di affinare le tecniche investigative attraverso cui poter acquisire una grossa mole di informazioni. Da qui la ricerca di un ragionevole punto di equilibrio tra tutela della riservatezza ed esigenze accertative nella perenne conflittualità tra autorità e libertà del cittadino.

Janus faced: authority and freedom in data retention. About a recent ruling of Court of Cassation.

The progress of computer science has allowed to refine the investigative techniques through which to acquire a large amount of information, sometimes strictly confidential, of the person. It calls for a reasonable balance to be struck between the protection of confidentiality and the need for verification. And in this context, the perennial conflict between authority and the freedom of the citizen is constantly repeated.

SOMMARIO: 1. Le *crypto-chat* al vaglio della Corte di legittimità. 2. Impulsi d'oltralpe e recepimenti nazionali. 3. Sequestro informatico e copia del contenuto: le occasioni sprecate per dipanare contrasti irrisolti. 4. Garanzie e rimedi. 5. Letture alternative a presidio della riservatezza.

1. *Le crypto-chat al vaglio della Corte di legittimità*. Nelle più recenti pronunce nomofilattiche si rinviene il dibattito avente ad oggetto l'impiego delle nuove tecniche investigative che consentono di acquisire uno sterminato patrimonio informativo, attraverso la decifratura di sistemi crittografati o la sorveglianza occulta dei *personal devices*.

La principale questione concerne, da un lato, la riconducibilità di tali attività captative entro i confini di una normativa tipizzata e, dall'altro, la tutela delle garanzie delle parti.

E dinanzi a nuove metodiche investigative[1], il giurista, ancor prima del Legislatore, è chiamato ad interrogarsi sull'utilizzabilità nel processo delle indagini espletate mediante *encrypted communication platforms* e, soprattutto, sul loro inquadramento giuridico.

[1] Allo stesso modo, può ricordarsi la strada battuta dalla giurisprudenza di legittimità in tema di investigazioni per il tramite del captatore informatico. Ancor prima dell'intervento legislativo, è stato il giudice di legittimità a definire i confini entro i quali poter legittimare l'inoculazione del *virus* informatico (cfr. Cass., Sez. VI, 26 giugno 2015, n. 27100, in *Guida dir.*, 2015, 41, 83 ss.; Cass. Sez. VI, 6 aprile 2016, n. 13884, in *Dir. inf. e informatica*, 2016, 1, 81; Sez. un., 1° luglio 2016, n. 26889, in *questa Rivista,* 2016, 2, 348 ss.; GRILLO- MOSCATO, *Riflessioni sulla prova informatica*, in *Cass. pen.*, 2011, 371. Per un approfondimento, si veda ATERNO- CAJANI – COSTABILE – MATTIUCCI – MAZZARACO – GRASSO- VULPIANI, *Computer forensics* e *indagini digitali. Manuale tecnico – giuridico e casi pratici*, Forlì, 2011.

Anche se si è passati dal captatore informatico al c.d. *IMSI Catcher*[2], non si è ancora pienamente acquisita la consapevolezza che nel mondo virtuale è l'etere digitale a costituire il nuovo *spazio* da esplorare, in cui si collocano e transitano le informazioni potenzialmente utili, ma non tutte, alle indagini.
L'impiego diffuso dei *social network*[3] e degli *smartphone*[4], che consentono di trattenere una grossa mole di dati personali, nonché i sistemi di *cloud computing*[5] hanno contribuito all'emersione di tutte quelle metodiche investigative riconducibili all'acronimo di *data retention*[6]: espressione che si riferisce all'acquisizione e al trattenimento dei dati suscettibili di costituire prova digitale[7], con una forte intrusività nella sfera privata altrui.
Nel contesto attuale, gran parte delle proprie informazioni, inerenti alla vita personale e non, sono rintracciabili dai *social*: al di là della congerie di dati in concreto acquisibili attraverso lo spionaggio dai *social network*, è certamente dai dati privati che possono trarsi le informazioni più rilevanti[8].
Invero, per quanto riguarda le modalità di "apprensione", l'acquisizione di dati pubblici attraverso il ricorso alla c.d. *Open Source* non pone particolari problemi, almeno *prima facie*, trattandosi di attività atipica, riconducibile agli artt. 55 e 348 c.p.p. Il mutamento di prospettiva si ha ponendosi nella rinnovata dimensione costituzionale e convenzionale della *privacy*, che svela l'inadeguatezza del parametro dell'idoneità accertativa e della tutela della libertà morale (art. 189 c.p.p.) a cui si ricorre per legittimare l'accesso ad una vasta gamma di informazioni.

---

[2] CURTOTTI – RIZZI – NOCERINO – RUSSITTO – GILIBERTI- SCARPA, *Piattaforme criptate e prova penale,* in *Sist. Pen.*, 2023, 6, 173 ss. Per ulteriori approfondimenti, CAMON, *Il cacciatore di IMSI*, in *questa Rivista*, 2020, 1, 1 ss.; NOCERINO, *Il tramonto dei mezzi di ricerca della prova nell'era 2.0*, in *Dir. pen. proc.,* 2021, 1017 ss.

[3] CONTI- TORRE, *Spionaggio informatico nell'ambito dei social network, in Le indagini atipiche*, a cura di Scalfati, Torino, 2014, 395 ss.: gli Autori approfondiscono il tema della c.d. *on-line surveillance* e il controllo occulto sulle piattaforme social mediante il programma spia *O-Sint*, con uno sguardo comparatistico alla giurisprudenza costituzionale tedesca.

[4] TESTAGUZZA, *Digital forensics. Informatica giuridica e processo penale*, Studi raccolti da Giarda-Spangher- Tonini, 2014, 2; o, ancora, BENE, *Il pedinamento elettronico: truismi e problemi spinosi,* in *Le indagini atipiche*, a cura di Scalfati, 347 ss.

[5] LA MUSCATELLA, *La ricerca delle fonti di prova sulle reti di cloud computing: le nuove frontiere delle investigazioni digitali tra profili giuridici e questioni operative*, in *Cib. dir.*, 2013, 477 ss.

[6] LUPARIA, *Privacy, diritto della persona e processo penale*, in *Riv. dir. proc.*, 2019, 1464.

[7] GAITO-VALENTINI, *Stato senza diritto e difesa smaterializzata: la sostanziale inutilità del diritto alla prova,* in *questa Rivista*, 2021, 2 ss.

[8] CONTI- TORRE, *op. cit.,* 547 ss.

La soluzione esegetica mi sembra non solo poco orientata alla tutela della riservatezza, ma anche non pienamente conforme ai canoni di determinatezza e prevedibilità, giacché non è possibile identificare *ex ante* le modalità operative e i limiti attraverso cui avvenga l'attività di captazione.

La vicenda assume contorni ancora più problematici con riguardo all'acquisizione di dati non pubblici allocati sui *social networks*, trattandosi di attività che si serve, sovente, della cooperazione tra Stati[9]. Ed è proprio in questo contesto, che si rivengono le recentissime frontiere investigative rappresentate dalle piattaforme di comunicazione criptate, tra cui *Encrochat* e *Sky-Ecc*[10], impiegate dalle organizzazioni criminali internazionali per pianificare, soprattutto nel narcotraffico, i propri affari.

I *cryptophones*, anche definiti *Dedicated Encrypted Communication Devices (DECD)*, sono degli *smartphone* che consentono di svolgere operazioni, chiamate o tenere conversazioni, senza possibilità di intercettazione o pedinamento satellitare: trattasi, almeno in apparenza, di un sistema impermeabile al controllo[11]. Con l'utilizzo di tecniche di indagine, ancora in via di sperimentazione, le autorità investigative francesi, con la cooperazione internazio-

---

[9] GAITO, *Rogatorie*, in *Procedura penale*, a cura di Dominioni- Corso- Gaito- Spangher-Galantini-Filippi- Garuti-Mazza- Varraso-Dinacci- Bontempelli- Mancuso- Iasevoli, Torino, 2023, 1173 ss.; VALENTINI, *L'acquisizione della prova tra limiti territoriali e cooperazione con autorità straniere*, Padova, 1988.

[10] Si tratta di sistemi crittografati scoperti dall'attività investigativa comune svolta, tra il 2020 e il 2021, dalle Autorità giudiziarie e di Polizia di Francia, del Belgio e dei Paesi Bassi. Cfr. *Comunicazione della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni empty. Strategie dell'UE per la lotta alla criminalità organizzata 2021-2025,* in https*://eur-lex.europa.eu/legal-content. EncroChat* era una Rete di comunicazioni e un fornitore di servizi con sede in Europa che offriva *smartphone* modificati consentendo comunicazioni crittografate tra gli abbonati. Il servizio di messaggistica crittografata *EncroChat* e i relativi telefoni personalizzati sono stati scoperti dalla gendarmeria francese nel 2017 che, poco dopo, ha provveduto a disattivare la piattaforma. *Sky Global* era una rete di comunicazioni e un fornitore di servizi con sede a Vancouver, in Canada: uno dei suoi prodotti più importanti era l'applicazione di messaggistica sicura *Sky ECC* e i criptotelefoni. Il 9 marzo 2021 Francia, Belgio ed Olanda, attraverso un'attività di indagine svolta a seguito della costituzione, sul canale giudiziario, di una squadra investigativa comune, sono riusciti a violare i *server* sui quali sono conservate le comunicazioni. Per ulteriori approfondimenti in materia di *chat* criptate, CURTOTTI- RIZZI- NOCERINO- RUSSITTO- GILIBERTI- SCARPA, *Piattaforme criptate e prova penale,* in *Sist. Pen.,* 2023, 6, 173 ss.

[11] Nei criptofonini vengono disabilitati i servizi facilmente penetrabili, tra cui la localizzazione *GPS*, i servizi *Google*, il *bluetooth*, la videocamera o fotocamera, i microfoni, oltre ad essere inibito l'uso di schede SD. Rimangono attive le chiamate ma solo in modalità *VoIP* (*Voice over IP*), senza l'uso della rete GSM. Per ulteriori approfondimenti, cfr. MORCELLA, *La vicenda dei criptofonini in attesa della decisione della Cassazione,* in *www.ilpenalista.it,* 2023.

nale e il coinvolgimento della Procura europea[12], sono riuscite ad acquisire informazioni attraverso l'apprensione in blocco di tutti i dati contenuti nei criptofonini, fornendo una chiave di cifratura comune che ha permesso di decriptare dati altrimenti non decifrabili. La legittimità costituzionale di queste tecniche è stata confermata dal *Conseil costitutionnel*[13].

I nuovi sistemi hanno interessato anche l'autorità giudiziaria interna: da qui l'interesse per i recenti approdi della Cassazione in materia di trattenimento delle informazioni attraverso la decriptazione delle piattaforme *Encrochat* e *Sky-Ecc.* In particolare, i giudici di legittimità, sollecitati dai difensori, sono chiamati a definire i limiti processuali delle modalità di apprensione dei dati allocati su *server* stranieri[14].

Sul versante dell'inquadramento giuridico, si è ritenuto che le informazioni dai sistemi *Encrochat* e *Sky-Ecc* vengano acquisite con due diverse tecniche: in un primo caso, si procede a captare le conversazioni, così da applicare la disciplina di cui all'art. 266-*bis* c.p.p., mentre, in un secondo caso, si acquisiscono dati dopo aver decriptato, ricorrendo così alle previsioni di cui agli artt. 234 ss. c.p.p. In quest'ultima ipotesi, si procede alla richiesta ad uno Stato europeo di trasmettere, previa decriptazione, messaggi di comunicazione e dati già conservati presso il *server*.

Sulla base di tale ragionamento, la Corte, seguita dai giudici di merito, guardando al tipo di dato acquisibile, ha concluso per la riconducibilità dell'attività investigativa atipica alla disciplina dell'apprensione di documenti conservati all'estero (art. 234-*bis* c.p.p.), facendo leva sulla circostanza che le informazioni fossero già state assunte e decifrate dall'autorità straniera[15].

---

[12] Cfr. MORCELLA, *op. cit.*; CAMALDO - DI PAOLO-DIDDI- GALANTINI- MARCOLINI- ZANETTI, *Processo penale e regole europee: atti, diritti, soggetti e decisioni*, vol. II, a cura di Ruggeri, Torino, 2018; MARCHETTI- SELVAGGI, *La nuova cooperazione giudiziaria penale. Dalle modifiche al Codice di procedura penale alla cooperazione giudiziaria penale*, coordinato da Barrocu, Milano, 2019.

[13] *Conseil costitutionnel*, n.2022-987, Q.p.c. del 8/04/2022.

[14] In questi casi, i difensori degli imputati hanno richiamato l'attenzione della Corte di legittimità talvolta sulla violazione delle norme in materia di intercettazione, talaltra sulla lesione del contraddittorio circa le modalità di apprensione delle *chat* allocate sui server esteri. Cfr. Cass., Sez. IV, 18 aprile 2023, n. 16348, Papalia, *inedita*; Cass., Sez. I, 15 settembre 2022, n. 34059, Molisso, *inedita*; Cass., Sez. VI, 20 dicembre 2022, n. 48330, Rv. 284027; Cass., Sez. I, 15 febbraio 2023, n. 6364, Rv. 283998; Cass., Sez. I, 15 febbraio 2023, n. 6363, Minichino, *inedita*.

[15] Cass., Sez. IV, 28 aprile 2023, n. 17647, Gulluni, *inedita*; Cass., Sez. IV, 18 aprile 2023, n.16348, Papalia, *inedita*; Cass., Sez. IV, 18 aprile 2023, n.16345, Liguori +3, *inedita*; Cass., Sez. I, n.34059 del 15 settembre 2022, Molisso, *inedita*; conf. Cass., Sez. VI, 20 dicembre 2022, n.48330, Rv. 284027; Cass., Sez. I, 15 febbraio 2023, n.6364, Calderon, Rv. 283998; Cass., Sez. I, 15 febbraio 2023, n.6363, Mini-

A destare perplessità è l'impostazione metodologica seguita dalla Cassazione ogni qualvolta si debba inquadrare giuridicamente una tecnica captativa di informazioni: la ricostruzione tipizzante viene diversificata a seconda della tipologia dei dati in concreto appresi, ignorando che le procedure di *data retention* sono tutte accomunate dalla lesività della sfera privata altrui.

Sul piano delle garanzie[16], si è riconosciuta all'interessato soltanto la possibilità di conoscere le documentazioni che attestino le modalità con cui si è svolta la decriptazione, al fine di poterne verificare la validità[17]. Secondo l'orientamento interpretativo, ad oggi maggioritario[18], la compatibilità di tali procedure con il diritto di difesa non sarebbe frustrata dalla scelta di mettere a disposizione delle parti soltanto i risultati acquisiti e non anche il percorso attuato per giungere all'acquisizione, posto che l'autorità giudiziaria straniera abbia verificato il regolare rispetto delle sequenze acquisitive del dato informatico.

Purtroppo, è doveroso prendere atto che soltanto in un precedente giurisprudenziale[19] il Supremo Consesso ha sostenuto che gli elementi di prova assunti mediante il ricorso alle *encrypted platforms* fossero inutilizzabili in quanto lesivi del diritto di difesa. In questa pronuncia, degna di nota, si è affermato che il principio del contraddittorio impone una dialettica procedimentale non soltanto sugli esiti del materiale acquisito, ma anche sulle modalità attraverso cui si procede. In buona sostanza, la difesa gode del diritto di accedere alla documentazione dell'attività investigativa svolta e di conoscere le modalità con cui sono stati rinvenuti i messaggi criptati, in virtù dell'osservanza del diritto di contraddittorio. La pronuncia è rimasta, però, isolata, prediligendosi l'itinerario intrapreso dall'orientamento maggioritario che svilisce le prerogative inviolabili del giusto processo.

E proprio con riguardo ai diritti dell'interessato a fronte dell'acquisizione di informazioni dai sistemi di *chat* criptate, la Prima Sezione della Corte di cas-

---

chino, *inedita*. Nella giurisprudenza di merito, cfr. Corte Ass. di Roma, sent. n.7 del 9 giugno 2022, imp. Nesci; Trib. Roma, sez. Riesame, ord. del 16 settembre 2022; Trib. Reggio Calabria, Sez. Riesame, ord. del 12 ottobre 2022.

[16] Cass., Sez. IV, 25 giugno 2020, n.19216, Ascone, *Rv.* 279246-01. In tal senso, Cass., Sez. V, 26 ottobre 2016, n.45002, Crupi, Rv. 268457; Cass., Sez. V, 12 gennaio 2017, n.1405, Ruso, Rv. 269015; Cass., Sez. I, 26 maggio 2009, n.21673, Pizzata, Rv. 243796; Cass., sez. II, 1° luglio 2010, n.24776, Mutari, Rv. 247750.

[17] Cass. Sez. IV, 7 settembre 2022, n. 32915, Lori, *inedita*.

[18] In questi termini, Cass., Sez. I, n. 6363, *cit.*

[19] Cass., Sez. IV, 7 settembre 2022, n.32915, *cit.*

sazione è intervenuta di recente [20], con l'obiettivo di ridisegnare il perimetro operativo di tale attività. Più specificamente si è ribadito che l'acquisizione di informazioni attraverso i nuovi sistemi di crittografia richieda un sindacato da parte del giudice interno del solo rispetto dei principi fondamentali, fermo restando una presunzione di legittimità dell'attività svolta e «(...) la competenza del giudice straniero in ordine alla verifica della correttezza della procedura e all'eventuale risoluzione di ogni questione relativa alle irregolarità riscontrate».

È, dunque, a carico dell'interessato l'onere di provare, sulla base di specifici elementi, l'irregolarità delle operazioni e l'incompatibilità con i principi fondamentali. L'eccessiva gravosità dell'onere si evince dall'asimmetria delle parti in punto di disponibilità di tecniche investigative, richiedendo all'interessato conoscenze ultra-specialistiche concernenti i sistemi di decriptazione impiegati.

Va anche detto che la ricostruzione esegetica non ignora il problema di attribuire una veste giuridica ad un'attività dai contorni fumosi, ma non si spinge ad individuare punti fermi in un ambito poco incline a preservare la riservatezza.

I giudici di legittimità, con affermazioni petitorie, si sono limitati a sottolineare l'esigenza di un controllo interno ad opera dei giudici domestici circa il rispetto dei principi fondamentali, per poi riconoscere una presunzione di legittimità di tali attività captative, attribuendo al giudice straniero il compito di verificarne la correttezza. Nessun riferimento, neppure attraverso la tecnica dell'*obiter dictum*, al bisogno di preservare la riservatezza a fronte di una tecnica investigativa che può andare ben oltre l'acquisizione di dati strettamente pertinenti alle indagini.

Anzi, al di là di affermare, in modo più solenne che pragmatico, che tali attività debbano osservare «i principi fondamentali», senza specificare la latitudine di tale espressione, la Corte ne afferma la presunta legittimità, con un sindacato rimesso al giudice straniero, ignorando che la verifica circa l'utilizzabilità dei dati acquisiti dovrebbe spettare al nostro interprete, quale custode di quel nucleo duro di diritti fondamentali, di matrice costituzionale, che ineriscono alla dignità della persona.

[20] Cass., Sez. I, 5 maggio 2023, Costacurta, Rv. 284440-01. In tal senso, Cass., Sez. I, 27 aprile 2023, De Rosa, *inedita*.

A ben vedere, e la giurisprudenza di legittimità lo dimostra, persiste ancora in materia la differenza, scivolosa, tra *lex loci* e *lex fori*, secondo cui è regola generale che la prova acquisita in territorio estero sia disciplinata dalle norme processuali vigenti nello Stato in cui è stata assunta, mentre vale la c.d. *lex fori* per ciò che riguarda la sua utilizzabilità ed efficacia dimostrativa. Sono regole di comune buon senso, prima ancora di essere normativizzate, giacché nel momento in cui l'atto debba produrre i suoi effetti nel procedimento pendente, sarà la legge dello Stato, presso cui è instaurato il procedimento, a regolamentarlo[21]. Ciò vuol dire che, qualora l'atto investigativo sia stato assunto all'estero, ma venga utilizzato nell'ordinamento interno, dovrà risultare conforme ai principi e ai valori tutelati a livello costituzionale, pena la sua inefficacia dimostrativa.

Ebbene, dalle decisioni nomofilattiche emerge una certa priorità accordata alla c.d. *lex loci*, atteso che si riconosce una presunzione di legittimità dell'operazione la cui regolarità è sottoposta al controllo esclusivo del giudice straniero. Sebbene la Corte abbia precisato che l'unico limite da osservare sia il rispetto dei principi fondamentali, perviene poi a ritenere prevalenti le norme processuali vigenti in fase acquisitiva, affermazione, quest'ultima, non condivisibile, giacché finisce per svilire la differenza tra fase acquisitiva e fase di controllo.

Si tratta di una riflessione ancorata all'insegnamento, vetusto ma mai realmente superato, della Corte costituzionale[22] la quale, con affermazione *tranchant*, distingue tra nome che disciplinano l'acquisizione delle prove e norme che ne disciplinano l'utilizzabilità, non potendosi ritenere che le prove assunte in conformità ai principi internazionali siano per ciò stesso utilizzabili, dovendo altresì rispondere agli *standard* di tutela predisposti dal tessuto costituzionale dello Stato richiedente.

Se ciò è vero, sarebbe necessario mutare l'angolo di osservazione in tema di acquisizione dei dati digitali allocati in *server* stranieri: ai fini della loro utilizzabilità, essi dovrebbero essere *in primis* conformi ai valori assiologici dello Stato costituzionale, dovendo spettare al giudice interno, dinanzi al quale si deciderà per l'utilizzabilità o meno dell'atto investigativo, la verifica circa la regolarità di tali procedure.

---

[21] GAITO, *op. cit.,* 1189 ss.

[22] Corte cost., n. 379 del 1995.

Non si vuole sostenere che qualsiasi atto acquisito all'estero non rispondente alle modalità operative dell'ordinamento domestico sia per ciò stesso non utilizzabile: tuttavia, occorre verificare che gli atti assunti "oltre confine" siano quantomeno rispettosi degli *standard* minimi di tutela del diritto all'equo processo, del diritto di difesa e, soprattutto, del diritto all'autodeterminazione della persona.

Per supplire il vuoto legislativo, la giurisprudenza si auto-legittima un ruolo nomo-poietico e, divenendo creativa, ridefinisce l'impiego di mezzi investigativi atipici, cercando di prevenire o almeno di attenuare la compromissione dell'intimità altrui, nonché di riequilibrare, per quanto possibile e con i limiti derivanti dall'esercizio della *iurisdictio*, un sistema fragile. Dunque, *de iure condito*, si auspica che gli interpreti intavolino una riflessione più attenta sugli atti acquisiti attraverso il ricorso a rogatorie internazionali e si soffermino sul terreno scivoloso della distinzione tra *lex loci* e *lex fori*, sì da garantire che la verifica di legittimità spetti al giudice domestico, soggetto soltanto alla *lex fori* e orientato alla salvaguardia delle garanzie inviolabili.

Invero lo sforzo interpretativo di ricondurre entro confini tipizzati le tecniche investigative che si servono del progresso tecnologico[23] non è mai stato realmente portato a termine, considerato che il tema della *data retention*, sotto le vesti delle più disparate modalità acquisitive, torna ciclicamente all'attenzione dei giudicanti.

A conferma di ciò, si può far cenno al tentativo di ricostruzione ermeneutica delle nuove attività di localizzazione tramite navigatore satellitare[24] o di acquisizione di contenuti *e-mail*.

Quanto alle tecniche di pedinamento satellitare, la giurisprudenza nomofilattica ha avvertito la necessità di attribuire uno statuto giuridico a tale attività, ricorrendo, come spesso accade, al contenitore della prova atipica[25].

---

[23] Di PAOLO, *Acquisizione dinamica dei dati relativa all'ubicazione del cellulare ed alter forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense*, in *Cass. pen.,* 2008, 3, 1219 ss.; SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.,* 2012, 580 ss.; STRAMAGLIA, *Il pedinamento satellitare: ricerca ed uso di una prova "atipica"*, in *Dir. pen. proc.*, 2011, 213 ss.

[24] BENE, *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali*, in *Le indagini atipiche,* a cura di Scalfati, Torino, 2014, 443 ss.

[25] Cass., Sez. IV, 7 giugno 2022, n. 21856, Rv. 283386; Cass., Sez. II, 27 maggio 2019, n. 23172, Rv. 276966; Cass., Sez. III, 27 febbraio 2015, Rv. 264519; Cass., Sez. 2, 13 febbraio 2013, n. 21644, Rv. 255541; Sez. I, 17 aprile 2012, n. 14529, *inedita*. In dottrina, CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007, 239; DI PAOLO, *"Tecnologie del controllo" e prova pena-*

Analoghe per tutte le attività captative sono le perplessità e i dubbi di compatibilità con il principio di stretta legalità, di proporzionalità e di tutela dei diritti fondamentali della persona: in particolare, anche con riguardo all'acquisizione dei contenuti *e-mail*, si discute circa la riconducibilità giuridica ad un'attività tipizzata ovvero alla categoria residuale della prova atipica[26].
L'esigenza di assicurarsi celermente il contenuto dell'*e-mail*, evitandone la dispersione o l'alterazione, induce a ricondurre giuridicamente l'attività entro i confini dell'accertamento tecnico ripetibile[27], da svolgere nelle forme di cui agli artt. 359 e 360 c.p.p. Tuttavia, un simile approdo garantirebbe all'interessato di partecipare all'accertamento, sì da poter esercitare adeguatamente il diritto di difesa: per tale ragione, considerato che l'acquisizione dei contenuti e-*mail* avviene in modo tendenzialmente occulto, altra tesi sostiene la riconducibilità dell'attività entro i confini dell'intercettazione ai sensi dell'art. 266-*bis* c.p.p[28].
In realtà, un conto è captare flussi di comunicazioni, ben altro è accedere direttamente nel *server* in cui transitano e sono conservate tutte le comunicazioni degli utenti: evidente è, pertanto, il *discrimen* rispetto all'attività intercettativa che consente "soltanto" captazioni mirate e circoscritte[29].
Dinanzi al bisogno di ricondurre ad una disciplina tipizzata le diverse modalità di captazione dei dati, due sono le alternative di metodo: in un primo caso, si procede a diversificare il trattamento legislativo applicabile a seconda del

---

le. L'esperienza statunitense e spunti per la comparazione, Padova, 2008, 252 ss; PERNA, *Mezzi atipici di ricerca della prova nell'attività di polizia giudiziaria: videosorveglianza, pedinamento e localizzazione satellitare*, in *Riv. polizia*, 2007, 672; STRAMAGLIA, *Il pedinamento satellitare: ricerca ed uso di una prova "atipica"*, in *Dir. pen. proc.,* 2011, 214.

[26] L'emancipazione dell'indagine digitale dall'investigazione ordinaria è dovuta alla L. 18 marzo 2008 n.48, cit. In dottrina, MANCUSO, *L'acquisizione di contenuti e-mail,* in *Le indagini atipiche*, a cura di Scalfati, Torino, 2014, 497 ss.; LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cyber crime [l. 18 marzo 2008, n. 48]*, a cura di Luparia, 2009, 141-142.

[27] In senso conforme, CURTOTTI, *Rilievi e accertamenti*, Padova, 2013, 183; LAGI, *L'accertamento tecnico ripetibile. La gestione del reperto informatico*, in *Cybercrime – Diritto e procedura penale dell'informatica,* a cura di Cadoppi- Canestrari- Manna- Papa, 2023, 1477 ss. Nella giurisprudenza, merita un richiamo Cass., Sez. I, 4 giugno 2009, n.23035, Corvino, *Rv.* 244454; nonché Cass., Sez. I, 18 marzo 2009, n. 11863, Ammutinato, *Rv.* 243922.

[28] ZACCHÉ, *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.*, 2013, 4, 109. Sul punto, PITTIRUTTI, *Profili processuali della prova informatica*, in '*Incontri ravvicinati' con la prova penale. Un anno di seminari a Roma Tre*, a cura di Marafioti- Paolozzi, Torino, 2014, 59.

[29] MANCUSO, *op. cit.*, 516 ss.

tipo di dato acquisito; in un secondo caso, più rispettoso dei diritti fondamentali, si guarderà all'invasività dell'attività captativa in sé considerata per individuare una normativa organica cui riferirsi.
Seguendo il primo approccio, si distinguono i dati segreti (oggetto di conversazioni via *social*) da quelli pubblici (rispetto ai quali non si pongono particolari problemi in punto di riservatezza) e, infine, da quelli riservati: per quanto concerne i primi si va a captare il contenuto dei messaggi ricevuti ed inviati, applicando il *corpus* di norme in tema di intercettazioni telematiche (art. 266-*bis* c.p.p.)[30].
Qualora, invece, si tratta di dati riservati, il trattamento giuridico sarà affine a quello della prova atipica, con provvedimento motivato ad opera del pubblico ministero e senza necessaria autorizzazione giurisdizionale.
Diversa la soluzione qualora si ponga l'attenzione sul tipo di attività posta in essere: a ben vedere, l'opzione di differenziare il trattamento giuridico a seconda del tipo di dato acquisito non è coerente con il bisogno di garanzia dei diritti fondamentali della persona. Tuttavia, la differenziazione del regime oscura la matrice comune di tali tecniche investigative e, cioè, l'invasività delle attività captative di elementi digitali. Non corre, infatti, alcuna concreta differenza tra l'acquisizione di schermate *chat* o l'acquisizione di dati afferenti, ad esempio, ai *file*, contenuti nel *device*, o alle chiavi di accesso ad *account* personali: comune denominatore è, e resta, l'invasività dell'attività acquisitiva rispetto al nucleo intangibile di diritti fondamentali sanciti, oltre che dalle Carte internazionali, dagli artt. 14 e 15 Cost.
De iure condito, l'unica disposizione applicabile resta quella in tema di prove atipiche (art. 189 c.p.p.): occorre, a rigore, verificare *ex ante* l'idoneità accertativa dell'atto e la sua non incidenza sulla libertà morale, rimettendo poi alle parti e all'interprete la definizione delle modalità con cui si procede.
Tuttavia, poiché, come si è cercato di evidenziare, le nuove tecnologie investigative, nonostante le indiscusse potenzialità di successo[31], finiscono per comprimere indebitamente diritti fondamentali dei singoli, la norma di cui all'art. 189 c.p.p. sarebbe inidonea, in quanto generica, ad attuare la riserva di legge

[30] TORRE, *Il captatore informatico, Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017.
[31] CAPONE, *Intercettazioni e Costituzione. Problemi vecchi e nuovi,* in *Cass. pen.*, 2017, 3, 1263 ss.: l'A., pur non mettendo in discussione l'utilità di tali strumenti, ne evidenzia le problematiche, creando un ponte di collegamento tra le tradizionali modalità investigative (intercettazioni di flussi di comunicazioni) e i moderni strumenti di indagine che sfruttano le nuove tecnologie.

e ad impedire l'impiego di mezzi di prova lesivi delle prerogative inviolabili della persona[32].
In assenza e in attesa di un quadro giuridico di riferimento, essendo la normativa vigente obsoleta rispetto alle nuove sfide imposte dall'era digitale, disorienta l'atteggiamento ondivago della giurisprudenza che è passata dal ricondurre nell'alveo della prova atipica alcune attività investigative, all'inquadrare l'acquisizione dei dati attraverso lo spionaggio sui *social* nell'ambito delle intercettazioni telematiche, sino ad arrivare, da ultimo, a sostenere che i dati conosciuti attraverso le tecnologie di decriptazione siano assimilabili ai documenti assunti all'estero a norma dell'art. 234-*bis c.p.p.*
L'oscillazione giurisprudenziale è determinata da un vizio di metodo: la modulazione del trattamento giuridico alla luce della diversa tipologia del dato acquisibile. Da qui la necessità di un intervento legislativo volto a definire, in modo puntuale, le modalità operative di questi nuovi atti investigativi[33], apprestando un'organica disciplina alla luce della costante pervasività che connota le nuove tecniche di *data retention*[34].

2. *Impulsi d'oltralpe e recepimenti nazionali.* La *querelle* in ordine allo *status* giuridico della prova digitale non si è mai del tutto assopita e continua a suscitare l'interesse del diritto vivente.
A causa dell'alto grado di tecnicismo richiesto per l'acquisizione delle prove digitali[35], si è sovente ricondotta quest'ultima nell'alveo delle prove scientifiche[36].

---

[32] CONTI- TORRE, *op. cit.,* 535 ss.
[33] Sul punto, già in tempi ormai risalenti rispetto alle recenti frontiere digitali, cfr. ANGELONI, *In tema di videoregistrazioni, prove atipiche*, in *Giur. it.*, 2009, 1521 ss.
[34] CORTE EDU, 26 aprile 1979, *Sunday Times* c. *Regno Unito*, in cui si specifica l'esigenza di rendere qualsiasi interferenza nei diritti fondamentali altrui «ragionevolmente preventivabile».
[35] 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, 4509, secondo cui la prova digitale è definita una «*slippery form of evidence*», giacché presenta peculiarità tali da far dubitare della sua riconducibilità alle disposizioni codicistiche.
[36] MARAFIOTI, *op.* cit., 4510. Secondo NOVARIO, *Le prove informatiche*, in *La prova penale*, a cura di Ferrua- Marzaduri -Spangher, Torino 2013, 123, le prove informatiche sono riconducibili «alla categoria delle prove tecniche o scientifiche, quali prove derivate dall'impiego di tecnologie informatiche». In questi termini, LORUSSO, *La prova scientifica*, in *Prova penale e metodo scientifico*, a cura di Catalano-Curtotti Nappi- Della Monica- Lorusso- Montagna- Procaccino, Torino, 2009, 26; cfr. TONINI, *La prova scientifica: considerazioni introduttive*, in *Dir. pen. proc.*, 2008, 8. In giurisprudenza, Cass., Sez. IV, 17 settembre 2010, Cozzini, in *Dir. pen. proc.*, 2011, 1341 ss., con nota di Tonini.

Se, per un verso, la riqualificazione della prova digitale in termini di prova scientifica consente un maggiore controllo sulle modalità operative impiegate, al contempo l'evanescenza della categoria, nonché l'impiego di strumenti tecnologici ad alto potenziale intrusivo sono indici che fanno propendere per uno statuto *ad hoc*, evitando delle sovrapposizioni che possono provocare equivoci in punto di disciplina applicabile[37].

Sulla scia dell'esperienza anglo-americana, gli organi investigativi hanno individuato delle linee guida "domestiche" al fine di standardizzare le procedure da seguire nella *data retention*. Esse però, oltre a non avere efficacia vincolante, sono connotate da un elevato tasso di discrezionalità; sicchè per lungo tempo ogni organo investigativo ha finito per adottare delle proprie metodiche[38], ciò inevitabilmente pregiudicando l'esigenza di coerenza sistematica.

A fronte del silenzio del Legislatore e all'assenza di indicazioni univoche concernenti le *best practices*, va posta in debito risalto anche la mancata previsione di rimedi sanzionatori.

Sul tema, le soluzioni prospettate sono tutt'altro che univoche: si è ravvisata, ad esempio, un'ipotesi di inutilizzabilità dei dati acquisiti in violazione delle linee guida[39], che mal si concilia con la natura duttile e non vincolante delle *stesse*. Si potrebbe al più ipotizzare un sindacato ad opera del giudice circa l'utilizzabilità degli elementi di prova acquisiti in difformità delle linee guida e senza garantire l'integrità dei dati, con il rischio di indebite disparità di trattamento.

Da qui la necessità di un intervento legislativo che specifichi le *guidelines*[40] e che individui altresì i rimedi in caso di violazioni delle stesse. Si auspica, inoltre, che anche gli interpreti, nell'opera costante di diritto vivente, siano inclini

---

[37] RICCI, *Digital evidence, sapere tecnico-scientifico e verità giudiziale*, in *Dir. pen. proc.,* 2010, 348

[27] LUPARIA- ZICCARDI, *Le «migliori pratiche» nelle investigazioni informatiche: brevi riflessioni sull'esperienza italiana,* in *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea*, a cura di Cajani- Costabile, Forlì, 2001, 211.

[39] VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. dell'Internet,* 2008, 509: l'A. ritiene possa configurarsi una nullità di regime intermedio. *Contra*, LORENZETTO, *Le attività urgenti di investigazione informatica*, in *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime, a cura di Luparia, Milano, 2009, 163*: l'A. sostiene che, considerati i limiti imposti dal principio di tassatività delle nullità, si potrebbe ravvisare l'inutilizzabilità dei dati digitali acquisiti in violazione delle *best practices.*

[40] In senso opposto, cfr. DANIELE, *Caratteristiche della prova digitale*, in *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, a cura di Ruggieri- Picotti, 2011, 211.

ad assumere una posizione uniforme e in grado di bilanciare le esigenze di conservazione ed acquisizione dei dati con il bisogno di tutelare la dignità della persona.

La ricerca di un punto di equilibrio è stato un tema spesso affrontato anche, e soprattutto, dalla Corte di giustizia dell'U.E.[41] nell'ottica di assicurare prevalenza ai diritti fondamentali censiti dalla Carta di Nizza: si tratta di decisioni[42], che, da un lato, rafforzano la tutela del diritto alla riservatezza e, dall'altro, segnano un'evidente frattura nell'odierna società tecnologica, giacché si tenta di porre limiti all'utilizzo generalizzato e spesso disinvolto della rete informatica.

Nella vicenda della c.d. *data retention*[43], la C.G.U.E. ha dichiarato l'invalidità della direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006, riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione, per violazione del principio di proporzionalità desumibile dagli artt. 7,8, 52 par. 1 Carta dei diritti fondamentali dell'Unione Europea. Le criticità riguardano l'assenza di limiti oggettivi all'obbligo indiscriminato di conservazione delle informazioni informatiche e l'omessa predisposizione di sanzioni di inutilizzabilità del materiale probatorio acquisito in modo illecito.

Successivamente, la Grande camera è tornata sul tema con una dirompente pronuncia[44] con cui ha dichiarato possibile l'acquisizione dei dati, limitandola ai soli procedimenti per gravi reati ed ha stabilito che è necessario l'intervento di un'autorità pubblica, terza rispetto a quella richiedente l'acquisizione[45].

---

[41] Corte giust. UE, sent. 24 novembre 2011 (C-70/10) e 16 febbraio 2012 (C-360/10), nonché, in termini parzialmente diversi, Corte giust. UE, sent. 27 marzo 2014 (C-314/12).

[42] Si veda, ad esempio, Corte EDU, Sez. III, 30 maggio 2017, *Trabajo Rueda vs Spagna*.

[43] Corte giust. UE, sent. 8 aprile 2014, *Digital Rights Ireland Ltd.*, con nota di FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?, in Dir. pen. cont.,* 2014.

[44] Corte giust. UE, sent. 2 marzo 2021, (C- 746/18). In dottrina, v. STEFANO, *La Corte di giustizia interviene sull'accesso ai dati di traffico telefonico e telematico e ai dati di ubicazione a fini di prova nel processo penale: solo un obbligo per il legislatore o una nuova regola processuale?,* in *Cass. pen.,* 2021, 2556 ss.; Cfr. LEO, *Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici*, in *Sist. Pen.,* 2021; SPANGHER, *I tabulati: un difficile equilibrio tra esigenze di accertamento e tutela di diritti fondamentali,* in *www.giustiziainsieme.it,* 2021.

[45] GAETA, *Consensi e dissensi sulla indipendenza del p.m. (a proposito del potere di acquisire i tabulati telefonici*), in *questa Rivista*, 2021, 3.

I *dicta* della Corte di giustizia hanno aperto una breccia anche nel sistema interno, giacché il Legislatore ha tentato, sia pure con scarsi risultati, di addivenire ad una disciplina organica riguardante l'acquisizione e la conservazione di dati digitali: per quanto si sia sforzato di individuare precisi limiti operativi[46], permane tutt'oggi una conservazione indiscriminata degli stessi, ciò provocando inevitabilmente tensione con i principi affermati dalla Corte.
Primo passo verso la ricostruzione normativa della materia si è avuto con l'art. 132 cod. *privacy* (d.lgs. 196/2003)[47], che prevede l'obbligo di conservazione per ventiquattro mesi dei dati informatici o telefonici: su questa disciplina, si è innestata la modifica di cui al d.l. n.354 del 2003[48] che ha disposto che l'acquisizione delle informazioni avvenga con decreto motivato del giudice, adottato su richiesta del pubblico ministero o delle parti private.
Le modifiche legislative, tuttavia, sono state piuttosto incerte: ad opera della l. n.155/2005[49] si è nuovamente introdotto il potere del pubblico ministero di acquisire tutte le informazioni conservate dal fornitore, così imboccando una deriva inquisitoria con l'accentramento di poteri di controllo e gestione dei dati digitali in capo alla pubblica accusa.
Al fine di recepire le istanze provenienti dalle Corti europee – che hanno spinto verso il maggiore riconoscimento del diritto alla segretezza dei dati –, il d.lgs. n.101 del 10 agosto 2018 ha novellato l'art. 132 cod. *privacy*, dando attuazione al c.d. "pacchetto europeo di protezione dei dati personali"[50]: si è previsto l'obbligo di conservazione dei dati telefonici per ventiquattro mesi e dei dati relativi al traffico telematico per dodici mesi[51].
Atteso che la norma consente la conservazione indiscriminata dei dati telefonici o informatici per l'accertamento di qualsiasi reato, parte della dottrina ha

---

[46] CERQUA, *La circolazione dei dati contenuti nei tabulati telefonici*, in *La circolazione della prova nell'Unione Europea e la tutela degli interessi finanziari,* a cura di Camaldo - Bana, Forlì, 2011, 291 ss.
[37]Cfr. Codice in materia di protezione dei dati personali, recante "Disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio", 27 aprile 2016, in *Gazz. Uff.*, 29 luglio 2003, n. 174, Suppl. ord. n. 123.
[48] Recante "*Disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia*", in Gazz. Uff., 29 dicembre 2003, n. 300. Il d.l. è stato convertito dalla L. 26 febbraio 2004, n. 45, in Gazz. Uff., 27 febbraio 2004, n. 48.
[49] "Misure urgenti per il contrasto del terrorismo internazionale", in Gazz. Uff., 27 luglio 2005, n. 173. Il d.l. è stato convertito dalla l. 31 luglio 2005, n. 155, in Gazz. Uff., 1° agosto 2005, n. 177.
[50] Il decreto legislativo ha dato attuazione al Regolamento (UE) 2016/679.
[51] PISATI, *Indagini preliminari e intelligenza artificiale: efficienza e rischi per i diritti fondamentali,* in *Proc. pen. giust.*, 2020, 4, 963 ss.

ravvisato un'irrimediabile tensione con gli artt. 7,8, 52 par. 1 della Carta di Nizza[52].

Pertanto, la disposizione doveva essere, ad avviso di molti[53], disapplicata, in quanto in contrasto con il diritto comunitario: si è auspicato, in tale prospettiva, il rinvio pregiudiziale alla Corte di giustizia per definire il dubbio di compatibilità dell'art. 132 cod. *privacy* con i diritti fondamentali sanciti dall'ordinamento comunitario[54].

Al fine di neutralizzare le critiche, il Legislatore è nuovamente intervenuto in materia di acquisizione dei dati, ricorrendo allo strumento, inflazionato negli ultimi tempi, della decretazione d'urgenza[55]: infatti, è stata limitata l'acquisizione dei dati ai soli procedimenti aventi ad oggetto reati più gravi, selezionati in base al trattamento sanzionatorio, affidando un controllo preventivo all'autorità giudiziaria e prevedendo la sanzione dell'inutilizzabilità dei dati, se acquisiti in violazione delle disposizioni di legge (art. 132 comma 3-*quater* cod. *privacy*)[56].

Rimasta inalterata è l'irragionevole differenziazione della durata dei tempi di conservazione: non si comprende perché, ad esempio, i dati relativi alle chiamate senza risposta vadano conservati per soli 30 giorni, considerato sia la loro utilità investigativa sia la difficoltà di acquisirli in un così breve arco temporale. Va, quindi, posta in debito risalto l'esigenza di uniformare le discipline.

A ciò si aggiunga anche che, pur circoscrivendo l'acquisizione dei dati ai reati più gravi, nessuna limitazione ha riguardato il tipo di informazioni assunte, non prescrivendo alcuna selezione preventiva tra elementi più o meno pertinenti a fini investigativi.

---

[52] SIGNORATO, *Novità in tema di data retention. La riformulazione dell'art. 132 codice privacy da parte del D.lgs. 10 agosto 2018 n.101,* in *Dir. pen. cont.*, 2018, 11, 153 ss.

[53] MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta.*, in *Cass. pen.,* 2, 2015, 760 ss. Per ulteriori approfondimenti, IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, in *Cass. pen.,* 2014, 4274 ss.; COLOMBO, *Data retention e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE,* in *Cass. pen.*, 2014, 2705 ss.

[54] FLOR, *op. cit.,* 178 ss.

[55] D.l. n.132 del 30 settembre 2021.

[56] LORENZETTO, *Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenitore al contenuto, passando per la copia,* in *Cass. pen.*, 2010, 4, 1522 ss.: l'A. aveva già prefigurato la sanzione dell'inutilizzabilità nel caso di acquisizione dei dati assunta in violazione delle norme in materia di genuinità della prova.

Sicchè, almeno *de iure condito*, si dovrà fare affidamento su una giurisprudenza consapevole dell'obbligo di interpretare le disposizioni conformemente ai principi costituzionali ed euro-unitari[57], limitando *ragionevolmente* la conservazione indiscriminata di dati digitali.
La prospettiva non è pienamente rassicurante sul piano dell'effettività della tutela dei diritti inviolabili: a dimostrazione dell'andatura altalenante degli orientamenti esegetici sono i recenti "approdi" in materia di *cryptochat*, considerato che, pur avendone la possibilità, la Corte di legittimità ha glissato sul bisogno di attenuare la forte intrusività provocata dai mezzi investigativi.
Pertanto, sarebbe necessaria un'opera compiuta del nomoteta che, abbandonata la tecnica dell'efficientismo, predisponga un'attenta normativa in tema di *data retention* con la previsione di limiti di durata equipollenti per tutti i dati e con l'individuazione di una finestra di controllo giurisdizionale all'interno della quale selezionare elementi di prova pertinenti e scartare quelli che, se conservati in maniera perdurante, possono inevitabilmente ledere il diritto di ciascuno alla propria intimità[58], alla stregua di quanto già accade per le intercettazioni.

3. *Sequestro informatico e copia del contenuto: le occasioni sprecate per dipanare contrasti irrisolti.* Sebbene il *vulnus* alla riservatezza desti maggiori preoccupazioni con riguardo agli strumenti investigativi privi di referenti normativi, esso rappresenta una costante che interseca anche le tradizionali tecniche di indagine: l'acquisizione di dati attraverso *software* di de-criptazione non ha fatto altro che far riemergere tutti quei nodi problematici, mai realmente sciolti, che riguardano, da tempo, le attività di perquisizione e sequestro dei supporti informatici.
È pacifico in dottrina e in giurisprudenza che il *discrimen* tra perquisizioni ed ispezioni riguardi il tipo di attività in concreto svolta: in particolare, le prime si

[57] Corte giust. UE, 5 aprile 2022, G.D., C-140/20, con nota di IOVENE, *Nuova decisione della Corte di giustizia in materia di tabulati: quali conseguenze per l'ordinamento nazionale?,* in *Cass. pen.,* 2022, 2363 ss. In argomento, v. FILIPPI, *La Corte di Lussemburgo ribadisce lo stop ai tabulati: una fine annunciata,* in *www.penaledp.it,* 2022; SAMBUCO, *Note in tema di data retention*, in *questa Rivista*, 2022, 2, 2 ss.
[58] PISATI, *Full collection of data e diritto di difesa*, in *Riv. it. dir. proc. pen.*, 2019, 2239 ss.: l'A. riprende alcune pronunce della Corte E.D.U., secondo cui la massa di milioni di dati contenuti nei supporti sequestrati «[...] by its nature [...] inevitably included a mass of data which was not prima facie relevant», ribadendo così la necessità di una selezione ad opera degli organi investigativi, così da limitare il numero «manageable proportions».

sostanziano in un'attività di ricerca, laddove le seconde si caratterizzano per essere attività di osservazione[59].
Ciò premesso, occorre adeguare la disciplina di entrambi i mezzi di ricerca della prova alla nuova realtà digitale e intercettarne le criticità.
Con riferimento alle ispezioni, mancando una normativa organica, è stata la prassi a legittimare tale attività su qualunque sistema o supporto informatico; per le perquisizioni, invece, ha provveduto in tal senso la legge n.48 del 2008[60], a condizione della conservazione e della non alterazione dei dati[61] (art. 247 comma 1-*bis* c.p.p.). Dunque, la *golden rule* in materia di perquisizioni informatiche è la conservazione dei dati, a prescindere che essi siano o meno pertinenti e funzionali alle indagini.
Tale proiezione finalistica è discutibile proprio sul piano delle prerogative della persona sottoposta alle indagini a fronte di un'indiscriminata, indistinta e generalizzata conservazione dei dati informatici. Non è stata presa in considerazione la tutela del singolo a fronte di attività altamente intrusive della sua intimità.
L'inizio dei lavori preparatori in seno alla Commissione Lattanzi poteva certamente essere un'occasione utile per fare ordine all'interno di una normativa caotica.
E, invece, nel dare attuazione alla c.d. Riforma Cartabia, il decreto legislativo n.150 del 10 ottobre 2022 si è limitato ad inserire una disposizione in materia di perquisizioni negative, cui, cioè, non sia seguito il sequestro[62].
L'intervento è stato sollecitato per colmare un vuoto legislativo, oggetto di censura da parte della Corte di Strasburgo[63], la quale ha ritenuto l'Italia responsabile per la violazione dell'art. 8, par. 2, della C.E.D.U.
Nel caso di specie, il ricorrente si era lamentato di non aver potuto ottenere un controllo giurisdizionale, preventivo o a posteriori, giacché nelle ipotesi in cui fosse stata osservata la consequenzialità tra perquisizione e sequestro, avrebbe potuto far valere le proprie doglianze attraverso la facoltà di proporre riesame, con tutti i limiti derivanti proprio dalla struttura del rimedio.

---

[59] BARGIS, *voce Perquisizione*, in *Dig. Pen.*, vol. IX, 1995, 501
[60] Cfr. CURTOTTI, *Rilievi e accertamenti tecnici*, Padova, 2013.
[61] FELICIONI, *Le ispezioni e le perquisizioni,* Milano, 2004, 47.
[62] Relazione Ufficio del Massimario, 2023, 2, 53 ss.
[63] Corte EDU, 27 settembre 2018, *Brazzi c. Italia.*

In particolare, è stato previsto, nei casi di perquisizione negativa, un inedito sindacato giurisdizionale, nelle ipotesi di perquisizione ad opera del pubblico ministero o della polizia giudiziaria.
Il nuovo istituto, ai sensi dell'art. 252-*bis* c.p.p., legittima la persona nei cui confronti la perquisizione sia stata disposta o eseguita a presentare opposizione avverso il decreto emesso dall'organo di pubblica accusa. Giudice competente a decidere sull'opposizione è il giudice per le indagini preliminari, il quale la accoglie qualora accerti che la perquisizione sia avvenuta «fuori dei casi previsti dalla legge».
Dunque, ed è questo un primo aspetto critico, i vizi deducibili con l'atto di opposizione sono soltanto quelli che si riversano nella violazione della legge, giacché soltanto in presenza di questi[64] l'intrusività nella libertà altrui non potrà essere tollerata. Si tratta però di una limitazione che esclude la sindacabilità nel merito di una perquisizione informatica fortemente invasiva.
Ben potrebbe accadere, infatti, che l'attività perquisitiva consenta all'autorità investigativa di entrare in possesso di una grossa mole di informazioni anche riservate: si pensi alle perquisizioni *on-line* sugli archivi *cloud* dell'interessato, ove spesso vengono conservate informazioni strettamente riservate e magari segrete.
Stando alla *littera legis*, qualora alla perquisizione legittima non segua il sequestro, l'interessato non avrà alcuno strumento da poter attivare, soprattutto qualora le informazioni acquisite siano del tutto non pertinenti alle indagini.
A lasciare perplessi poi è l'omessa predeterminazione degli effetti connessi all'accoglimento dell'atto oppositivo[65], che nella Relazione illustrativa del progetto di riforma è ricondotta all'orientamento giurisprudenziale secondo cui l'eventuale illegittimità dell'atto perquisitivo non produce effetti a cascata sul successivo eventuale sequestro.
In altri termini, il verbale che dispone la perquisizione, ancorché dichiarata in sede oppositiva illegittima, potrà conservare utilizzabilità probatoria ovvero potrà essere presupposto per l'adozione del conseguente provvedimento di

[64] In termini, Cass., Sez. III, 27 giugno 2013, n. 28151, P.M. in proc. Chifor, Rv. 255458: «Sono illegittimi i provvedimenti di perquisizione e sequestro probatorio operati di iniziativa dalla polizia giudiziaria oppure disposti dal pubblico ministero qualora non trovino giustificazione in una notizia di reato legittimamente acquisita o siano eseguiti in assenza di elementi idonei a configurare una specifica ipotesi di reato».
[65] GIALUZ, *Per un processo penale più efficiente e giusto. Guida alla lettura della riforma Cartabia (profili processuali), in Sist. Pen.,* 2022, 18.

sequestro[66]. Da qui l'inefficacia dell'accertamento di illegittimità della perquisizione.
La previsione pare claudicante sotto il profilo della ragionevolezza: in buona sostanza, non si vede perché l'interessato debba o abbia interesse a sollevare opposizione avverso un verbale che, comunque, continuerà ad essere utilizzabile. D'altronde, l'accertamento dell'illegittimità di un atto cui non seguono conseguenze pratiche non sembra essere una soluzione né logica né ragionevole sotto il profilo di effettività di tutela dei diritti. La sensazione è che il Legislatore abbia voluto "rattoppare" un difetto evidente e non tollerabile del sistema.
Stando così le cose, si è persa l'occasione di riforma per dare organicità ad una materia già di per sé difficile da inquadrare: indubbiamente si è fatto un piccolo passo in avanti verso il rafforzamento delle garanzie delle parti ma l'opportunità poteva essere meglio sfruttata per delineare un quadro completo di una disciplina che resta, ancora oggi, priva di garanzie e, soprattutto, priva di limiti a fronte della conservazione indistinta di dati personali. Permangono i riverberi distorsivi sulle situazioni soggettive protette come la riservatezza.
E se la portata lesiva di una simile attività può essere in parte attenuata in caso di mancato sequestro probatorio, inevitabile è l'effetto lesivo qualora alla perquisizione segua il sequestro di quegli stessi dati: la possibilità di invertire il rapporto tra perquisizione e sequestro nelle indagini digitali conferma che tra di essi non sussista un rapporto consequenziale, trattandosi di mezzi investigativi autonomi.[67]
Infatti, con l'affermarsi dell'era digitale, si sono ricompresi nel concetto di "cosa pertinente al reato[68]" i dati digitali: va ricordato, a tal proposito, che, prima della l. n. 48 del 2008, si dubitava della possibilità di sequestrare il con-

[66] Cass., Sez. I, 27 ottobre 2021, Cataldo, Rv. 282070.
[67] SIGNORATO, *op. cit.,* 221 ss. In giurisprudenza, sul rapporto tra perquisizione e sequestro, Cass., Sez. III, 10 maggio 2016, n.19365, Pirri; Cass., Sez. II, 29 marzo 2017, n.15784, Rv. 269856-01.
[68] Per un'analisi sul concetto di cosa pertinente al reato, si veda GABRIELLI, *Il sequestro probatorio non supera il riesame: la copia dell'hard disk ritorna al giornalista, sia pure con qualche "scorciatoia" argomentativa*, in *Giur. di mer. f.*, 4, 2007, 200. Di regola, la nozione corpo del reato si compone di due elementi: materialità e pertinenzialità al reato. Oggi, il concetto di materialità è largamente eroso a seguito della rivoluzione digitale: la liquidità del dato, dell'informazione o di ciò che è contenuto nel bene sequestrato ha preso il posto della materialità della *res*. Cfr. DEL POZZO, *voce Corpo del reato*, in *Enc. Dir.,* vol. X, Milano, 650. *In argumentiis*, RUGGERI- MAGGIO, *Il sequestro probatorio*, in *La prova penale,* a cura di Ferrua- Marzaduri- Spangher, Torino 2013, 785.

tenuto a prescindere dal contenitore, atteso che si negava che i dati potessero essere qualificati come elementi materiali e, dunque, cose[69].
L'equivoco di fondo era legato alla concezione di corpo del reato: la dottrina processual-penalistica ne evidenziava la necessaria fisicità, sicché appariva del tutto improprio qualificare come corpo del reato ciò che è, per natura, immateriale[70].
Successivamente, è maturata la consapevolezza che i dati digitali possano essere appresi a prescindere dal sequestro del supporto informatico in cui sono contenuti[71]. Su questa scia, la legge n. 48 del 2008 ne ha ammesso l'acquisizione, chiarendo che essi costituiscono forme di corrispondenza, suscettibili di sequestro, ai sensi dell'art. 254 c.p.p.[72], attraverso la materiale apprensione dell'intero supporto contenente le informazioni interessate.
Il trattenimento dei dati informatici può avvenire anche senza procedere al sequestro probatorio, mediante la tecnica c.d. *bit a bit*[73], che consente di creare la copia forense dell'originale[74].
Per quanto concerne lo *status* giuridico della copia forense, essa è stata[75] qualificata in termini di atto ripetibile: tuttavia, occorre distinguere i casi in cui avvenga a dispositivo spento ovvero acceso.
Nel primo caso, sarà considerata attività ripetibile, senza che ciò pregiudichi le esigenze di conservazione e autenticità, purché effettuata conformemente alle *best practices*.
Nel caso in cui, invece, l'acquisizione avvenga su dispositivi accesi, si tratterebbe di atti irripetibili: ne conseguirebbe, *mutatis mutandis*, l'applicazione

---

[69] DANIELE, *op. cit.,* 204.
[70] MONTI, *La nuova disciplina del sequestro informatico*, in *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime*, a cura di Luparia, Milano, 2009, 199.
[71] VACIAGO, *Le investigazioni telematiche*, in *Computer crime. Casi pratici e metodologie investigative dei reati informatici*, a cura di Piccinini- Vaciago, Bergamo, 2008, 102.
[72] MACRILLÒ, *Le nuove disposizioni in tema di sequestro probatorio e di custodia e assicurazione dei dati informatici*, in *Dir. dell'Internet*, 2008, 514.
[73] FASOLIN, *La copia dei dati informatici nel quadro delle categorie processuali*, in *Dir. pen. proc.,* 2012, 372 ss.
[74] Sulle tecniche di copia attraverso il c.d. *bit a bit*, si veda, per maggiori approfondimenti, COSTABILE, *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008,* in *Ciberspazio e dir.*, 2010, 500 ss.
[75] Cass., sez. III, 8 luglio 2015, n.29061, *Rv.* 264572-01, che ha affermato il principio di diritto secondo cui «[...] non integra un accertamento tecnico irripetibile l'estrazione dei dati archiviati in un computer, trattandosi di operazione meramente meccanica, riproducibile per un numero indefinito di valore».

della disciplina di cui all'art. 360 c.p.p., compendiata da plurime garanzie, tra cui la facoltà per la persona sottoposta alle indagini di formulare richiesta di incidente probatorio[76].
Si tratta di garanzie che mal si conciliano con l'esigenza, prioritaria per il Legislatore, di procedere nell'immediatezza alla copia dei dati, pena l'alterazione o la perdita degli stessi: si preferisce, pertanto, eludere la possibilità di un incidente probatorio, così da evitare un contraddittorio (anticipato), quale luogo elettivo di formazione della prova.
Ne consegue un'evidente tensione con i canoni del giusto processo, con l'indefettibilità del contraddittorio e con la garanzia della riservatezza: vietare la possibilità di un contraddittorio anticipato sulla formazione della prova per dare risalto e priorità alle istanze di non adulterazione del dato significa comprimere la facoltà per l'indagato di interloquire sulle informazioni da apprendere[77].
Ancora una volta, chiave di lettura dovrebbe essere quella di un ragionevole bilanciamento tra opposte esigenze: da un lato, l'esigenza di procedere nell'immediatezza all'acquisizione mediante tecnica *bit a bit* e, dall'altro, quella di preservare la *privacy* e di garantire uno spazio in cui poter dialogare circa la pertinenzialità al reato di tutte quelle informazioni che costituiscono patrimonio conoscitivo di una persona, alla stregua di un D.N.A. attraverso cui risalire alla sfera intima di ciascuno.

4. *Garanzie e rimedi.* In merito alla scansione procedurale caratterizzata dal sequestro del contenitore e perquisizione del contenuto, il sistema riflette un'evidente tensione in punto di tutela delle prerogative difensive per quanto concerne l'interesse ad impugnare ed esperire il riesame per la restituzione della copia dei dati digitali acquisiti[78] .
Non si dubita della possibilità di chiedere il riesame per ottenere il dissequestro del dispositivo informatico: il problema riguarda, tuttavia, la possibilità di disporre, in modo esclusivo, della copia ottenuta attraverso la materiale apprensione del supporto.

---

[76] In questo senso, cfr. PISATI, *op. cit.*
[77] LORENZETTO, *op. cit.*, 1522 ss.
[78] BARTOLI, *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature,* in *questa Rivista*, 2018, 1, 2 ss.

La Cassazione[79] ha cercato di porre fine ad un dissidio interpretativo in ordine alle garanzie difensive spettanti all'interessato a fronte del mancato riottenimento dei dati duplicati: le diverse tesi prospettate si fondavano sulla sussistenza o meno di un nesso eziologico tra sequestro e perquisizione.
In particolare, nella giurisprudenza maggioritaria[80] aleggiava l'idea secondo cui la copia dei dati fosse provvedimento a sé stante, del tutto separato dal sequestro precedente, di talché al singolo veniva preclusa la possibilità di accedere al riesame, considerato che il successivo dissequestro del supporto informatico determinasse il venir meno dell'interesse a proporre gravame.
In altre pronunce, si riconosceva un'interdipendenza tra sequestro e attività perquisitiva: senza sequestrare la *res*, non si sarebbe potuto duplicare i dati digitali, sicché i vizi del primo ricadevano sulla seconda attività; o addirittura, si è riconosciuto un diritto alla restituzione dei dati oggetto di acquisizione, consentendo, in entrambe le ipotesi, il controllo giurisdizionale in caso di mancata restituzione dei cloni.
Con il mutato quadro legislativo, nonostante il riconoscimento giuridico alla copia dei dati digitali, la giurisprudenza[81] è stata ferma sulle posizioni più restrittive, giungendo ad affermare che, avvenuto il dissequestro della *res*, venga meno l'ulteriore interesse ad impugnare per riottenere la disponibilità dei dati duplicati.
L'oscillazione giurisprudenziale non si è tuttavia arrestata: da ultimo si è pervenuti ad attribuire un autonomo *status* giuridico alla copia dei dati digitali.
Scandita la diversità ontologica tra sequestro del supporto informatico e perquisizione dei contenuti, v'era in giurisprudenza un indirizzo atto a riconoscere la facoltà di riesame soltanto in presenza di una perdita valutabile per il titolare del bene, dovendo essergli altrimenti negata[82].

---

[79] Cass., Sez. un., 7 settembre 2017, Andreucci, Rv. 270497-01.
[80] Cass., Sez. VI, 1° settembre 1994, n. 2682, *Marini*, Rv. 199141.; Cass., Sez. VI, 14 settembre 1998, n. 1331, Pomenti, Rv. n. 211590; Cass., Sez. VI, 7 luglio 1998, n. 2073, p.m. in proc. Colasante, Rv. 212219; Cass., Sez. II, 30 aprile 1999, n. 1480, Ferrari, Rv. 213306; Cass., Sez. II, 30 gennaio 2006, n. 3598, Canzano, Rv. 233335; Cass., Sez. II, 27 giugno 2007, n. 24958, Cal, Rv. 236759; Cass., Sez. II, 13 agosto 2007, n. 32881, Sandalj, Rv. 237763. Cass., Sez. III, 19 giugno 2000, n. 384, Motta, Rv. 217687; Cass., Sez. VI, 4 settembre 2003, n. 35087, Bonaduce, Rv. 226753.
[81] Cass., Sez. un., 7 gennaio 2008, n.230, Normanno, Rv. 237861.
[82] Cass., Sez. VI, 10 giugno 2015, n.24617, *Rizzo*, in *Giur. It.,* 2015, 1503 ss., con nota di LORUSSO, *Sequestro probatorio e tutela del segreto giornalistico*, in *Dir. pen. cont.*, 2015. In dottrina v, *ex multis*, CERQUA, *Ancora dubbi e incertezze sull'acquisizione della corrispondenza elettronica,* in *Arch. nuova*

Altro orientamento[83], invece, riconosceva il diritto di rivolgersi al giudice per ottenere la restituzione del bene per il solo fatto che permanesse un vincolo sui dati duplicati: d'altronde, non sarebbe stato ragionevole apprestare garanzie soltanto per recuperare il bene e non anche, e soprattutto, per riottenere i dati ivi collocati, giacché si sarebbe attribuita priorità al contenitore piuttosto che al contenuto.

Recependo il contrasto ermeneutico, le Sezioni unite sono intervenute nell'ottica di dipanarlo. L'alternativa posta all'attenzione della Corte è secca: per un verso, non sarebbe necessario estendere il riesame qualora fosse deputato soltanto a tutelare la proprietà della *res* sequestrata; per altro verso, qualora il riesame fosse rimedio funzionale a soddisfare garanzie di più ampio respiro, tra cui la tutela della riservatezza, spetterebbe all'interessato un diritto al controllo giurisdizionale per riottenere la piena ed esclusiva disponibilità del patrimonio informativo[84].

È maturata, finalmente, la consapevolezza dell'importanza di assicurare la disponibilità esclusiva del patrimonio conoscitivo. Inoltre, vengono differenziate le modalità di controllo giurisdizionale: qualora si tratti di copia ottenuta mediante la tecnica *bit a bit*, permanendo il vincolo, si seguiranno le regole proprie del riesame. Qualora, invece, si tratti di un dato-documento, essendo avvenuta la restituzione del supporto, si considera venuta meno la facoltà di proporre impugnazione, salvo che si deduca un interesse concreto e specifico ad ottenere l'esclusiva disponibilità del patrimonio informativo. Tuttavia, non è pacifico il riconoscimento del riesame in caso di mancata restituzione del dato-clone. In primo luogo, non si comprende come il destinatario dell'attività debba provare di avere interesse all'esclusiva disponibilità del patrimonio informativo e, in secondo luogo, cosa si intenda per "esclusiva disponibilità del patrimonio informativo". Né si comprende in che modo l'interessato possa provare di aver subito un pregiudizio dalla mancata restituzione di dati duplicati[85].

---

proc. pen., 2016, 269 ss.; COSTANZI, *Perquisizione e sequestro informatico. L'interesse al riesame nel caso di estrazione di copie e restituzione dell'originale*, in *Cass. pen.,* 2016, 286 ss.

[83] Cass., Sez. III, 21 settembre 2015, n. 38148, Cellino, con nota di ZAMPERINI, *Impugnabilità del sequestro probatorio di dati informatici,* in *Dir. pen. proc.,* 2016, 508 ss.

[84] BARTOLI, *op. cit.,* 2 ss.

[85] TODARO, *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare: revirement delle Sezioni Unite*, in *Dir. pen. cont.*, 2017, 1, 160.

Alla luce di ciò, la giurisprudenza successiva ha cercato di rendere nitidi i confini di un'espressione vaga: in parziale continuità rispetto a quanto già affermato, ha chiarito che l'interesse alla disponibilità esclusiva del dato informatico sussista di per sé, non dovendo l'istante dimostrare in positivo gli elementi da cui desumere ciò[86]. In buona sostanza, è sufficiente che esso si ricavi dagli atti processuali: si ammette, così, una presunzione di interesse ad impugnare a favore del destinatario delle attività captative.

È dubbio se l'interesse all'esclusiva disponibilità del patrimonio informativo sia accostabile alla riservatezza *tout court*: in realtà, volendo fornire un'interpretazione garantista, deputata ad innalzare la soglia di tutela dei diritti fondamentali, si ritiene che l'esclusiva disponibilità del patrimonio informativo sottintenda il concetto di *privacy* che, nonostante ciò non sia pacifico, può essere annoverato tra i diritti fondamentali[87] grazie al filtro dell'art. 2 Cost.

A ben vedere, l'estensione del diritto di azionare il rimedio del riesame genera tensioni con il principio di tipicità dei mezzi di impugnazione. Se si aderisse alla tesi secondo cui il riesame è consentito anche per il ri-ottenimento della copia clone e non solo per il dissequestro, si andrebbe ben oltre la *littera legis*, compromettendo, a dire di alcuni[88], la tassatività delle impugnazioni penali.

Per quanto tale interpretazione, a rigore, sia più rispettosa delle affermazioni della Corte di giustizia, essa si pone in frizione con i principi fondanti lo Stato costituzionale di diritto: in primo luogo, non consentire il riesame lede il principio della parità trattamentale, dal momento che si crea una forte disparità rispetto alla disciplina del sequestro, avverso il quale è possibile esperire il rimedio.

Il rischio è che, con l'occhio rivolto al diritto d'oltralpe e al bisogno di un'ermeneutica conforme, si finisca per svilire quelli che sono i capisaldi su cui si erge il nostro Stato costituzionale, squalificando garanzie fondamentali

[86] Cass., Sez. VI, 10 maggio 2022, n.18502, con nota di CASCONE, *La disponibilità esclusiva del dato informatico: una nuova pronuncia della Corte di Cassazione a tutela del "patrimonio informativo"* in *Cass. pen.*, 2023, 2, 555 ss.

[87] TODARO, *op. cit.*, 169: l'A. sostiene che, sebbene la *privacy* non rientri tra i diritti fondamentali sanciti dalla Carta costituzionale, giacché il problema della riservatezza non era avvertito ai tempi in cui è stato redatto il testo costituzionale, è indubbio che essa si annoveri tra i diritti di rango costituzionale con cui condivide il nocciolo duro, vale a dire la dignità della persona.

[88] SIGNORATO, *op. cit.,* 229.

che, ancor prima di trovare censimento nelle Carte internazionali, sono custodite nel testo costituzionale[89].
Aderire ad una tesi piuttosto che ad un'altra chiama in causa il criterio dell'interpretazione conforme, atteso che la lettura convenzionalmente orientata escluderebbe la possibilità di riesame, e, al contrario, una lettura costituzionalmente conforme condurrebbe l'interprete a riconoscere l'azionabilità di tale rimedio, in ragione dei possibili contrasti con il principio di eguaglianza.
È pacifico che se oggi si è innalzato lo *standard* di tutela dei diritti fondamentali, è merito – se non esclusivo, in buona parte – dell'integrazione con la giurisprudenza euro-unitaria e convenzionale: la commistione tra ordinamenti non deve, tuttavia, andare a detrimento di quelli che sono i principi fondanti il nostro Stato costituzionale[90].
Con riguardo al diritto di proporre riesame, andrebbe sostenuta un'interpretazione che, prima di essere aderente ai testi convenzionali, sia conforme ai precetti costituzionali: pertanto, il diritto andrebbe riconosciuto al fine di disporre della copia-clone, sì da garantire parità trattamentale con la disciplina del sequestro, salvaguardando altresì il diritto del singolo all'esclusivo godimento del suo bagaglio di informazioni.
L'ostacolo posto dalla *littera legis*, e, più in generale, dal principio di tassatività delle impugnazioni, potrebbe, dunque, essere superato attraverso l'opera ermeneutica, antidoto più potente alla fluidità del post-moderno.
Oggi si assiste ad un «progressivo disincanto nei confronti dell'assoluto primario teoricamente spettante alle norme di legge in materia penale, [...], in seguito alla scoperta delle più moderne teorie dell'interpretazione, specie di quelle di orientamento ermeneutico [...][91]»
La stessa giurisprudenza di legittimità, tornata in plurime occasioni sul tema, non ha mancato di ribadire che l'estensione delle garanzie debba essere svincolata da un aprioristico ossequio alla legge formale. Tra le garanzie riconosciute e predisposte a tutela della riservatezza, la Suprema corte[92] ha altresì

[89] RUOTOLO, *L'interpretazione conforme a Costituzione torna a casa*?, in *Consulta online*, 2019, 3, 589 ss.
[90] In argomento, IASEVOLI, *La Cassazione penale 'giudice dei diritti'. Tra chiusura al fatto e vincolo del precedente*, 2018, Napoli, *passim.*
[91] FIANDACA, *Sistema penale in transizione e ruolo del diritto giurisprudenziale*, Padova, 1997, 2 ss.
[92] Cass., Sez. VI, 4 aprile 2022, n. 12507; Cass., Sez. VI, 19 marzo 2021, n. 10815; Cass., Sez. VI, 2 dicembre 2020, n. 34265; Cass., Sez. II, 31 dicembre 2020, n.37941. In precedenza, si vedano: Cass.,

valorizzato il ruolo assunto dalla motivazione del decreto che dispone il sequestro del bene: per quanto essa possa essere concisa, deve dar conto delle finalità investigative perseguite, in conformità al principio di proporzionalità[93] e adeguatezza. Ancora, sempre nell'ottica di interpretare le disposizioni conformemente ai criteri di ragionevolezza e proporzionalità[94], si è riconosciuto che la durata del sequestro non possa essere indeterminata ma l'autorità giudiziaria, nello svolgere l'analisi dell'ingente massa di dati, dovrà disporre degli stessi nel tempo strettamente necessario per le attività investigative, dovendo poi procedere ad immediata restituzione degli stessi[95].

Pertanto, è illegittima un'acquisizione indiscriminata di dati informatici qualora non sia stato previamente adottato un provvedimento di sequestro che indichi il *fumus* di reato, il nesso eziologico con le informazioni da apprendere e le finalità per cui è strettamente necessario procedere a tale attività[96].

In definitiva, i giudici di legittimità ricostruiscono la disciplina della c.d. *data retention*, cercando di coordinare le esigenze investigative con la tutela di principi fondamentali[97], contribuendo così a formare quel nucleo di diritto vivente, viatico necessario affinché la *regula juris* sia sempre confacente alla «nostra vita pratica[98]».

A ben vedere, la frizione che subisce la tutela dell'intimità della sfera privata rispetto a sproporzionate e, talvolta, ingiustificate esigenze investigative è tutt'altro che risolta: a fronte di un simile stato di cose, occorre chiedersi

---

Sez. V, 4 aprile 2017, n. 16622, Storari; Cass., Sez. VI, 15 dicembre 2016, Amores, Rv. 268489; Cass., Sez. II, 12 aprile 2013, n. 16544, Verni; Cass., Sez. III, 7 luglio 2008, n. 27508, Rv. 240254.

[93] PALAZZO, Il *principio di proporzione e i vincoli sostanziali, in Principi, regole, interpretazione. Contratti e obbligazioni, famiglie e successioni. Scritti in onore di Furgiuele,* a cura di Conte- Landini, I, Mantova, 2017, 311 ss.

[94] IASEVOLI, *op. cit.,* 119-120.

[95] ALGERI, *Principio di proporzionalità e sequestro probatorio di sistemi informatici*, in *Dir. pen. proc.,* 2020, 849 ss.

[96] Cass., Sez. VI, 4 aprile 2022, n.12507, con nota di SCHILLACI, *Limiti del sequestro probatorio esteso a tutti i dati contenuti negli apparecchi telefonici o in altri sistemi informatici*, in *www.ilpenalista.it,* 2022.

[97] Cass., Sez. VI, 2 dicembre 2020, n. 34265, con nota di PITTIRUTI, *Dalla Corte di Cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus,* in *Sist. Pen.,* 2021. In dottrina, v. FONTANI, *Il sequestro probatorio di un documento informatico: bilanciamento tra esigenze investigative e baluardi difensivi,* in *Dir. pen. proc.*, 2022, 2, 236 ss; PARODI, *Perquisizioni e sequestri informatici e sequestri esplorativi: la S.C. delinea gli ambiti operativi*, in *www.ilpenalista.it*, 2021.

[98] RESTA, *Diritto vivente,* Bari- Roma, 2008, 32 ss.

quanto, e come, il solo mezzo del riesame sia adeguato all'esigenza di salvaguardare un interesse primario quale quello della riservatezza.
Il vaglio richiesto ai giudici competenti sarà di mera legittimità: o si riconosce l'illegittimità del sequestro e, dunque, esso viene meno, con conseguente restituzione dei dati digitali acquisiti oppure, e questo è l'esito che più desta preoccupazioni, il sequestro sarà considerato legittimo e non verrà disposta la restituzione delle copie.
I problemi sono però tutt'altro che risolti attraverso il riconoscimento, da parte del diritto vivente, della possibilità di proporre riesame per riottenere i cloni: ad essere non appropriato rispetto allo scopo di preservare l'indisponibilità esclusiva del patrimonio informativo è proprio il mezzo di gravame.
Già volgendo lo sguardo repentinamente alla disciplina del riesame, si possono notare i primi segnali di inadeguatezza: la procedura celere, scandita da tempi contingentati, presumibilmente non consentirà agli organi investigativi di analizzare tutto il materiale acquisito, discernendo ciò che è pertinente da ciò che non lo è.
Per tali ragioni, è necessario procedere ad una ridefinizione dei rimedi attivabili per godere della piena ed esclusiva disponibilità delle proprie informazioni[99]: si potrebbe, ad esempio, riadattare il modello dell'udienza stralcio per procedere repentinamente a separare i dati utili, rispetto ai quali comprensibile è il bisogno di conservazione, da quelli non proficui alle indagini[100].

5. Letture alternative a presidio della riservatezza. L'indagine sul tema della *data retention* muove da una premessa pacifica: qualunque sia il tipo di tecnica acquisitiva impiegata – dai sequestri informatici alle perquisizioni *on-line*, passando per il monitoraggio satellitare oppure per l'acquisizione di contenuti *e-mail*, sino ad arrivare ai *software* di decriptazione–, si realizza costantemente un prelievo generalizzato di una grossa mole di informazioni, di cui si è tentato di evidenziarne le tensioni con la tutela della *privacy* la quale, ab-

[99] CARNEVALE, *Copia e restituzione di documenti informatici sequestrati*, in *Dir. pen. proc.,* 2009, 481; LUPARIA, *op. cit.,* 375; SCHENA, *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*, in *Cass. pen.,* 2016, 306. In giurisprudenza, Cass., Sez. V, ord. 20 giugno 2016, n. 25527.
[100] IOVENE, *Perquisizione e sequestro di computer: un'analisi comparatistica*, in *Riv. dir. proc.*, 2012, 1616.

bandonata la dimensione puramente negativa («right to be let alone[101]»), è annoverata tra i diritti fondamentali della persona.
In generale, l'impiego degli strumenti tecnologici dovrebbe essere supportato da una consolidata normativa interna, non essere affidato, come invece accade, a fonti di rango internazionali o mere indicazioni di linee guida o, ancora, al formante giurisprudenziale.
Al contempo, tuttavia, preso atto della portata dirompente dei mezzi tecnologici, non si può pretendere che il Legislatore riesca zelantemente a stare al passo con l'evoluzione tecnologica, predisponendo puntuali e organiche discipline per ogni strumento che, oggi come in futuro, verrà impiegato nelle attività di indagini.
Negli ultimi tempi, si è tentato di rincorrere le innovate frontiere del digitale, apprestando, in modo peraltro confusionario e non efficace, una disciplina per ognuna di queste attività rientranti nella *digital evidence*. Un simile *modus procedendi* non ha fatto altro che provocare *caos* normativo, ciò ripercuotendosi sui diritti fondamentali della persona, oltre che sull'effettività di tutela, atteso che si è finito per normare alla rinfusa, senza pensare ad una disciplina organica sulle investigazioni digitali che possa fungere da baricentro per qualsiasi futuro sviluppo della *data retention.*
Con riferimento al sequestro del contenitore e perquisizione, e copia, del contenuto, si prende atto che l'esigenza di garantire l'autenticità e non modificabilità dei dati sia assurta a rango di principio fondamentale, prodromico al bisogno di completezza investigativa[102]: se il *fil rouge* delle disposizioni introdotte in via legislativa è rappresentato dal bisogno di integrità dei dati digitali, sembra che tale obiettivo si sia perseguito anche a costo di sacrificare le garanzie inviolabili della persona.
Nessun momento di garanzia, nessuna "pseudo" udienza di stralcio dei dati acquisiti non rilevanti, nessun contraddittorio[103] per l'accusato: sono tutte carenze legislative non compatibili con un sistema multilivello votato, almeno in principio, ad intensificare, non annichilire, la tutela dei diritti fondamentali.

---

[101] Tale definizione appartiene a WARREN-BRANDEIS, *The Right to Privacy*, in *Harward Law Review*, 1890, 4, 193.
[102] DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.,* 2011, 286 ss.
[103] Sull'esigenza di contraddittorio nell'acquisizione di dati digitale, v., *ex multis*, DANIELE, *op. cit.,* 286 ss.

I lavori preparatori confluiti, poi, nell'ampio progetto di riforma approvato con la L. n.134 del 2021 (Riforma Cartabia) potevano essere utile momento di confronto finalizzato a ridefinire le tecniche investigative in un'ottica costituzionalmente orientata. Tuttavia, con l'entrata in vigore della riforma, si è sprecata un'occasione utile e forse non così ripetibile per mettere mano ad una normativa la cui assenza non è più tollerabile, limitandosi il Legislatore ad ammettere la possibilità di opposizione in caso di perquisizione negativa che, come si è visto, non è esente da criticità.
Le carenze legislative finiscono per imporre l'intervento della giurisprudenza che ha tentato di ricostruire rimedi e garanzie in materia di sequestro e perquisizione dei supporti informatici, finendo talvolta per conferire priorità alle esigenze investigative, in spregio alla tutela della riservatezza.
In definitiva, fermo restando che nel diritto vivente è pacificamente riconosciuta la facoltà di proporre riesame per ottenere la restituzione dei dati duplicati, si nutrono dubbi con riguardo alla scelta di un mezzo di impugnazione improntato a tempi procedurali stringati, non compatibili con l'esigenza di analizzare la globalità dei dati e restituire quelli non pertinenti: sarebbe opportuno che il Legislatore preveda un controllo *ex ante* sui dati acquisiti, attraverso l'instaurazione di un apposito momento di contraddittorio partecipato, al fine di stralciare le informazioni non utili a fini investigativi.
Si potrebbe far ricorso alle finestre di giurisdizione, introdotte dalla c.d. Riforma Cartabia (d.lgs. n.150 del 2022)[104], sollecitando il giudice per le indagini preliminari a verificare la corretta qualificazione giuridica del fatto e la legittimità dell'acquisizione dei dati personali, così da evitare eccessive compressioni del diritto alla riservatezza e, al contempo, assicurando un contraddittorio anticipato in sede investigativa che consenta di acquisire soltanto dati realmente utili.
Per quanto concerne le altre tecniche investigative atipiche, si è cercato di sottolineare, sin dall'inizio, che principale criticità riguarda l'assenza di una normativa organica, cui ha cercato di supplire la giurisprudenza individuando, di volta in volta, la disciplina in concreto applicabile.
Tuttavia, il criterio, adottato dalla giurisprudenza, di individuare le disposizioni da impiegare a seconda del tipo di dato acquisito non tiene nella dovuta

[104] L'espressione "finestre di giurisdizione" viene generalmente utilizzata per definire i nuovi ambiti di intervento del giudice in spazi prima riservati al Pubblico Ministero. Cfr. MARANDOLA, *Le finestre di giurisdizione e il giudice del procedimento*, in *Proc. pen. giust.*, 2023, 1.

considerazione il comune denominatore di tali attività captative: trattasi di metodiche che, seppure in modo differente, consentono di assorbire una mole sterminata di informazioni e conversazioni.
Nell'ottica di un sistema multilivello di diritti, si auspica, invece, l'abbandono della metodologia di differenziazione basata sul tipo di dato, apprestando un'organica disciplina da impiegare per tutte quelle tecniche che, a prescindere dal tipo di informazione appresa, abbiano come obiettivo la c.d. *data retention*, non essendo possibile legittimare l'impiego dei diversi mezzi digitali attraverso interpretazioni estensive in una materia, peraltro, governata dal principio di tassatività.
Sarebbe, ad esempio, opportuno: a) stabilire *ex ante* le modalità attraverso cui ricorrere agli atti investigativi atipici, richiedendo una previa autorizzazione da parte dell'autorità giudiziaria sulla base di un'autonoma valutazione che tenga conto sia della gravità degli indizi sia delle esigenze che sollecitano l'utilizzo dei mezzi di indagine tecnologici; b) circoscrivere le attività ad alto potenziale intrusivo ai soli procedimenti per reati di cui agli artt. 51, comma 3-*bis* e 3-*quater* e 407, comma 2, lett. a, c.p.p.; c) prevedere la distruzione del materiale irrilevante attraverso l'istituzione di apposite "finestre di giurisdizione"; d) potenziare le procedure atte a garantire la corretta acquisizione dei dati e, infine, e) introdurre la sanzione dell'inutilizzabilità a fronte di modalità captative elusive del dettato legislativo e, prima ancora, del dettato costituzionale.
L'evoluzione irrefrenabile della *digital evidence* apre, oggi, la strada a nuove metodiche di indagine (basti pensare all'impiego, a tal fine, dei sistemi di intelligenza artificiale), in grado di comprimere ulteriormente i diritti dei singoli: per tali ragioni, si avverte, ancor di più, l'esigenza di un intervento del Legislatore che renda tollerabili, in una società di diritto, le limitazioni, da parte del pubblico potere, delle prerogative individuali della persona.
Pesa, e va considerato, l'insegnamento proveniente dalla Corte tedesca in tema di tutela delle garanzie inviolabili[105], secondo cui i diritti fondamentali della persona sono espressione del diritto alla libertà del cittadino nei confronti dello Stato.
Tali diritti possono essere limitati dal potere nella misura necessaria e proporzionata per la tutela di interessi pubblici: in uno Stato di diritto, la *golden rule* è, e resta, la libertà della persona, anche, e soprattutto, con riguardo al

[105] Cfr., CONTI- TORRE, *op. cit.,* 564.

mondo virtuale. Se ciò si traspone nel nostro ordinamento, il diritto del cittadino alla propria autodeterminazione nei riguardi della pubblica autorità resta la regola e, consequenzialmente, le limitazioni costituiscono l'eccezione.
Torna in auge il contrasto tra autorità e libertà.
La ricerca di un ragionevole punto di equilibrio tra potere pubblico e libertà personale, con riguardo all'uso di tecniche investigative invasive, impone una seria riflessione che vede coinvolti la giurisprudenza – dovendo essa prediligere una lettura della disciplina costituzionalmente orientata – e il Legislatore il quale, assumendosi la responsabilità di un assordante silenzio, dovrebbe predisporre una disciplina *ad hoc*, prescindendo da una differenziazione tra dati e optando, invece, per una normativa organica.
Nella consapevolezza che nei documenti, e oggi, soprattutto, nel *web*, è registrato il passato, «[...] e chi controlla il passato, controllerà il futuro[106]».

[106] ORWELL, *1984*, I, ed. originale, 1949.