UNIVERSITÀ DI TRENTO

INDAGINI E PROVE NELLA SOCIETÀ DIGITALE

QUESTIONI ATTUALI E PROSPETTIVE FUTURE

a cura di
GABRIELLA DI PAOLO
LUCA PRESSACCO

2025

UNIVERSITÀ DI TRENTO
Facoltà di Giurisprudenza

QUADERNI DELLA FACOLTÀ DI GIURISPRUDENZA

95

2025

Al fine di garantire la qualità scientifica della Collana di cui fa parte, il presente volume è stato valutato e approvato da un *Referee* interno alla Facoltà a seguito di una procedura che ha garantito trasparenza di criteri valutativi, autonomia dei giudizi, anonimato reciproco del *Referee* nei confronti di Autori e Curatori.

ISBN 978-88-5541-113-4
ISSN 2284-2810

Il presente volume è pubblicato anche in versione cartacea,
con il contributo della Facoltà di Giurisprudenza
dell'Università di Trento,
per i tipi di Editoriale Scientifica - Napoli
con ISBN 979-12-235-0292-1.

Giugno 2025

INDAGINI E PROVE NELLA SOCIETÀ DIGITALE

QUESTIONI ATTUALI E PROSPETTIVE FUTURE

a cura di
GABRIELLA DI PAOLO
LUCA PRESSACCO

Università degli Studi di Trento 2025

INDICE

Pag.

Gabriella Di Paolo
Prefazione 1

Gli Autori 3

Gabriella Di Paolo
Comunicazioni digitali e prova penale. Note introduttive 5

Alberto Camon
I confini mobili delle intercettazioni 9

Federica Iovene
I dati esterni delle comunicazioni: tendenze evolutive 27

Giulio Illuminati
Circolazione probatoria interna e transfrontaliera. Note introduttive 45

Luigi Giordano
La circolazione degli esiti delle intercettazioni in altri procedimenti interni. I riflessi della sentenza delle sezioni unite "Cavallo" sulla giurisprudenza successiva 53

Rosanna Belfiore
L'acquisizione transfrontaliera di prove digitali 81

Marianna Biral
Intercettazioni e tutela di terzi estranei al procedimento 97

Pag.

Fabio Cassibba
Indagini tecnologicamente assistite e tecniche investigative speciali. Note introduttive 115

Elisa Lorenzetto
I sequestri di smartphone*, dispositivi informatici e memorie digitali* 119

Silvia Signorato
La geolocalizzazione: tecniche e garanzie 139

Pasquale Bronzo
Le operazioni sotto copertura nel web 173

Jacopo Della Torre
Indagini penali e criptovalute 203

Antonino Alì
Backdoor *nei sistemi crittografici tra esigenze di sicurezza e diritti umani* 253

Luca Pressacco
Gli elementi di prova generati o raccolti tramite intelligenza artificiale. Considerazioni metodologiche 273

PREFAZIONE

Gabriella Di Paolo

Il presente volume raccoglie le relazioni e gli interventi svolti nel corso dell'incontro di studio «Indagini e prove nella società digitale. Questioni attuali e prospettive future», tenutosi a Trento il 26 e 27 settembre 2024, nell'ambito delle iniziative legate al Dipartimento d'eccellenza 2023-2027.

Il Convegno – organizzato dalla Facoltà di Giurisprudenza dell'Università di Trento in collaborazione con la Scuola Superiore della Magistratura (struttura didattica territoriale del Distretto di Corte d'Appello di Trento), sotto il patrocinio della Camera penale di Trento "Michele Pompermaier" e dell'Associazione italiana studiosi della prova (A.I.S.P.) – rappresenta l'ultimo di una serie di incontri dedicati alla materia probatoria, organizzati nel corso degli anni presso l'Ateneo tridentino. L'iniziativa nasce dall'esigenza, fortemente avvertita sia in accademia che dagli operatori del diritto, di dedicare un momento di riflessione e approfondimento ai numerosi e complessi problemi posti dal crescente impiego di metodi di indagine a caratura tecnologica in "ambiente digitale".

In questa prospettiva, la prima parte del convegno è stata dedicata alle intercettazioni e all'acquisizione dei dati esterni delle "comunicazioni" in senso stretto, anche nell'ottica della circolazione dei relativi risultati tra i procedimenti penali nazionali e transfrontalieri. La seconda parte dell'iniziativa, invece, ha riguardato metodi investigativi (come i sequestri di dispositivi informatici e la geolocalizzazione) e tecniche d'indagine speciali (come le operazioni *undercover* nella rete e le indagini per fatti di reato connotati dall'uso di criptovalute per finalità illecite) che incidono su diritti fondamentali, per così dire, di "nuova generazione". Ne è emerso un quadro articolato e composito, il cui filo conduttore può essere ravvisato nella convinzione che sia improcrastinabile l'elaborazione di uno statuto dei nuovi mezzi di ricerca della

prova adeguato alle peculiarità dell'ambiente digitale e della c.d. *electronic evidence*.

Nel licenziare le bozze del presente volume, desidero rivolgere un ringraziamento sincero a tutti coloro che hanno reso possibile lo svolgimento del Convegno all'interno degli Enti organizzatori, alle associazioni che vi hanno idealmente aderito concedendo il loro patrocinio nonché, e soprattutto, a tutti i relatori e interventori, per l'impegno profuso al fine di consentire una tempestiva pubblicazione degli atti. Ringrazio infine sentitamente la dott.ssa Marianna Biral e il dott. Luca Pressacco, che hanno impreziosito graficamente il presente volume con il loro attento e insostituibile lavoro di *editing*.

Trento, il 28 febbraio 2025
G.D.P.

GLI AUTORI

ANTONINO ALÌ, Professore Associato di Diritto internazionale – Università di Trento

ROSANNA BELFIORE, Professoressa Associata di Diritto processuale penale – Università di Catania

MARIANNA BIRAL, Ricercatrice di Diritto processuale penale – Università di Trento

PASQUALE BRONZO, Professore Associato di Diritto processuale penale – Università di Roma, *La Sapienza*

ALBERTO CAMON, Professore ordinario di Diritto processuale penale – *Alma Mater Studiorum*, Università di Bologna

FABIO SALVATORE CASSIBBA, Professore Ordinario di Diritto processuale penale – Università di Parma

JACOPO DELLA TORRE, Professore Associato di Diritto processuale penale – Università di Genova

GABRIELLA DI PAOLO, Professoressa Ordinaria di Diritto processuale penale – Università di Trento

LUIGI GIORDANO, Magistrato – Procura generale presso la Corte di Cassazione

GIULIO ILLUMINATI, già Professore Ordinario di Diritto processuale penale – *Alma Mater Studiorum*, Università di Bologna

FEDERICA IOVENE, Magistrato – Procura della Repubblica presso il Tribunale di Bolzano

ELISA LORENZETTO, Professoressa Associata di Diritto processuale penale – Università di Verona

LUCA PRESSACCO, Ricercatore di Diritto processuale penale – Università di Trento

SILVIA SIGNORATO, Professoressa Associata di Diritto processuale penale – Università di Padova

COMUNICAZIONI DIGITALI E PROVA PENALE

NOTE INTRODUTTIVE

Gabriella Di Paolo

Nell'aprire i lavori dell'odierno convegno, mi corre l'obbligo di sottolineare che esso rappresenta l'ultimo di una serie di incontri organizzati in materia probatoria presso la Facoltà di Giurisprudenza dell'Ateneo trentino. Ne ricordo qualcuno dei più recenti, giusto per fare esercizio di memoria storica: "Intercettazioni telefoniche tra riforme legislative fonica forense" (19 novembre 2020); "Intelligenza artificiale e processo penale. Indagini, prove e giudizio" (23 novembre 2020)[1]; "L'acquisizione di dati relativi al traffico telefonico/informatico o relativi all'ubicazione fra Codice Privacy" (13 maggio 2021), in cui si discuteva dei possibili riflessi nel nostro ordinamento della sentenza della Corte di giustizia del 2 marzo 2021, Prokuratuur[2]; "Questioni aperte in materia di tabulati telefonici" (5 ottobre 2022). Molti dei temi toccati in occasione dei pregressi incontri ritornano e si intrecciano, come ordito e trama, insieme ad altri, nel programma che scandisce le due giornate di questo convegno.

Non si tratta di un caso. Gli incessanti e rapidi progressi tecnologici del secolo breve[3] e la c.d. "transizione blu" hanno avuto riflessi signifi-

---

[1] Cfr. G. DI PAOLO, L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Napoli, 2022, accessibile anche in open access al seguente link: *https://iris.unitn.it/handle/11572/361122*.

[2] CGUE, grande sezione, sent. 2 marzo 2021, causa C-746/18, H.K. con l'intervento di Prokuratuur.

[3] La storia dell'umanità è da sempre una storia di progresso, ma negli ultimi due secoli l'evoluzione del sapere scientifico e della tecnica ha subito un'accelerazione che non trova pari in altre epoche storiche e che ha innescato profonde trasformazioni sociali, dei sistemi politici e dello stesso fenomeno giuridico. Cfr. S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997, 3 ss.;

cativi sull'amministrazione della giustizia penale e sulla funzione cognitiva del processo. Nel percorso guidato di conoscenza che connota il processo penale (e, ancora prima, la fase investigativa) al giorno d'oggi è inevitabile avere a che fare con metodi di indagine a caratura tecnologica e con "informazioni" (i c.d. dati) in formato digitale (la c.d. prova elettronica, *e-evidence*).

Si tratta di dati acquisiti con strumenti investigativi di varia natura, assai diversi per genesi e ubicazione: talvolta essi sono contenuti nei dispositivi personali (come smartphone, tablet o computer); talaltra, sono stoccati nei server di fornitori di servizi (*Internet Service Providers* (ISP) o altri *Providers*), i quali, fra l'altro, sono spesso collocati all'estero; in certi casi, la ricerca e l'acquisizione non riguarda dati "statici" (i c.d. dati freddi) – cioè dati precostituiti, conservati nelle memorie digitali – ma dati "in divenire", ovvero appresi in tempo reale, mentre vengono elaborati e/o sono in transito nella rete o nel web. Anche il *quid* rappresentato da tali dati è il più vario. Non si tratta più solo del "contenuto" delle comunicazioni. Oggi l'acquisizione può riguardare anche i dati "esterni" delle comunicazioni, dati che riguardano le transazioni finanziarie, le password digitate per l'accesso ai servizi, l'ubicazione sul territorio del dispositivo e del suo utilizzatore, le condizioni di salute e le attività fisiche (magari tracciate da dispositivi elettronici indossabili come *smartwatch* e *fitness watch*) della persona oggetto di sorveglianza, e così via.

Insomma, se per molto tempo le intercettazioni hanno rappresentato il principale mezzo investigativo tecnologicamente assistito, attualmente una grande mole di informazioni rilevanti per l'accertamento penale è reperita attraverso altri strumenti di ricerca della prova. E questo perché nella società digitale non c'è azione umana che non lasci una qualche traccia digitale. Opportunamente attrezzate, le autorità di *law enforcement* possono quindi avere accesso, in modo rapido e agevole, a una moltitudine eterogenea di dati apparentemente "innocui" o di limitata capacità dimostrativa se considerati singolarmente e isolatamente, ma in grado di restituire – se acquisiti, conservati ed elaborati comples-

---

M.R. FERRARESE, *Il diritto al presente. Globalizzazione e tempo delle istituzioni*, Bologna, 2002, 7 ss.

sivamente, anche attraverso l'uso di strumenti di intelligenza artificiale, – un profilo talmente preciso del soggetto interessato (e della sua vita privata) tale da equiparare o superare, per grado e qualità di intrusività, quella tradizionalmente annessa alle intercettazioni di comunicazioni.

Un altro aspetto degno di nota – questo è il secondo motivo che stimola l'approfondimento scientifico – è rappresentato dalla constatazione che di fronte alla già menzionata "fluidità" delle nuove tecniche investigative corrisponde frequentemente l'assenza di una specifica e compiuta disciplina normativa di riferimento.

L'evoluzione tecnologica – è risaputo – è molto più rapida del legislatore. Accade quindi spesso che le prassi investigative vengano sviluppate nel più assoluto vuoto normativo. E quando il legislatore interviene, lo fa in ritardo – come la nottola di Minerva, secondo la suggestiva immagine di Giulio Ubertis[4] – e con una tecnica normativa non sempre ineccepibile se non addirittura maldestra o lacunosa, tanto da rendere necessari ripetuti interventi sullo stesso oggetto: si pensi alle riforme e controriforme succedutesi nell'arco di pochi anni in materia di intercettazioni, oppure ai recenti interventi legislativi in materia di tabulati, frettolosamente varati in seguito di input sovranazionali.

In questa situazione di "anomia" è quasi inevitabile che la giurisprudenza (sia quella nazionale che quella delle corti europee) abbia finito per esercitare un delicato ruolo di "supplenza" del legislatore, con tutte le problematiche di carattere generale che ne discendono, a partire dalla crisi della legalità processuale (e dei principi di certezza del diritto e di conoscibilità e prevedibilità del legge) alla dubbia compatibilità costituzionale di tale "diritto giudiziario" con la divisione dei poteri e per di più in un ambito – come quello della compressione dei diritti fondamentali da parte dell'autorità – normalmente presidiato con la riserva di legge.

In considerazione di tale contesto e della continua evoluzione – una sorta di "moto perpetuo" – degli strumenti investigativi, il presente incontro è stato concepito come un'occasione per riprendere e approfondire alcune delle questioni maggiormente dibattute fra gli operatori del

[4] G. UBERTIS, *La prova scientifica e la nottola di Minerva*, in *Indice penale*, 2006, p. 501 ss.

diritto e gli studiosi. Tutto ciò con l'auspicio di offrire un contributo anche de *iure condendo*, ai fini della elaborazione di uno statuto legislativo idoneo rispetto alle peculiarità dei nuovi mezzi di indagine a contenuto tecnologico[5] nonché alle caratteristiche dell'ambiente digitale e delle "tracce elettroniche"[6] su cui insistono.

In quest'ottica, le sessioni di oggi pomeriggio saranno dedicate a temi più tradizionali quali le intercettazioni e l'acquisizione di dati esterni delle "comunicazioni" in senso stretto, anche nella prospettiva della circolazione dei relativi risultati tra procedimenti diversi. La giornata di domani toccherà, invece, metodi investigativi (come i sequestri di dispositivi informatici e la geolocalizzazione) e tecniche d'indagine speciali (come le operazioni *undercover* nella rete e le indagini per fatti-reato connotati dall'uso di criptovalute per finalità illecite) che incidono su diritti fondamentali, per così dire, di "nuova generazione".

[5] Segnatamente, il carattere potenzialmente indiscriminato della ricerca e i nuovi contenuti dei diritti di libertà sacrificati o compressi.

[6] Trattandosi di dati in formato elettronico, tali "tracce" sono immateriali, ubiquitarie e soprattutto volatili, con conseguente necessità di assicurare la catena di custodia, onde evitarne l'alterazione.

I CONFINI MOBILI DELLE INTERCETTAZIONI

Alberto Camon

SOMMARIO: *1. Il concetto di intercettazione e gli strumenti esclusi: cenni all'acquisizione dei dati di traffico. 2. Casi difficili. 3. Un paradosso. 4. L'innovazione tecnologica e la crisi del concetto di comunicazione: a) il "comportamento comunicativo". 5. Segue: b) i messaggi già arrivati. 6. Segue: c) gli scambi fra macchine. 7. Uno sguardo di sintesi sugli indirizzi della magistratura e sulle sue ideologie. 8. Prospettive.*

1. Il concetto di intercettazione e gli strumenti esclusi: cenni all'acquisizione dei dati di traffico

Fra le molte definizioni che dell'intercettazione sono state date, possiamo ricordare – per l'influsso che ha esercitato ed esercita sugli altri giudici – quella coniata dalle sezioni unite della Corte di Cassazione: una

> captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere altri e con modalità oggettivamente idonee allo scopo, attuata da soggetto estraneo alla stessa mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del suo carattere riservato[1].

La nozione spinge l'interprete a confrontarsi con due grandi aree tematiche. Una è composta dagli strumenti investigativi che stanno all'esterno di quel perimetro ma che sarebbe opportuno spostare all'interno. Toccheremo solo di sfuggita l'argomento, ma varrà la pena accennare a uno degli esempi più importanti: l'acquisizione dei dati sul traffico delle comunicazioni. Il legislatore lo tratta diversamente dalle intercettazioni perché, siccome il contenuto dei messaggi resta sconosciu-

[1] Cass., Sez. un., sent. 28 maggio 2003 n. 36747, Torcasio, in *CED Cass.*, n. 225465.

to, la lesione alla *privacy* sarebbe minore; ma il ragionamento, all'inizio accolto senza difficoltà, con l'andar del tempo ha incontrato resistenze crescenti.

Bisogna infatti considerare che disporre un'intercettazione significa mettere sotto controllo comunicazioni future; non si può intercettare un colloquio già svolto; l'unica maniera per raccogliere intorno a esso qualche informazione è proprio acquisire i tabulati. Almeno sotto questo profilo, l'acquisizione dei dati di traffico è più potente, riesce a spingersi in territori che sono invece inaccessibili alle intercettazioni.

Inoltre, è ormai diffusa la convinzione che l'analisi dei metadati delle comunicazioni, soprattutto quando abbraccia un arco di tempo ampio, può fornire un ritratto vivido, ricco di dettagli preziosi e spesso delicati: come ormai si usa dire, essa consente di "profilare" un individuo[2].

Infine, non sono rari i casi in cui anche il dato singolo, relativo cioè a una specifica comunicazione, svela molto, comunque più del contenuto.

> Immaginate un semplice messaggio di testo che recita: "qui". Il contenuto della comunicazione è vago e non rivela praticamente nulla. Qualcuno è da qualche parte. Ma cosa succederebbe se i metadati rivelassero che il messaggio è stato inviato da una donna in una clinica abortiva a un uomo a casa sua? Ecco che il quadro si fa chiaro. In questo caso, il contenuto del messaggio è molto meno intimo e rivelatore dei metadati[3].

Oppure pensiamo all'ipotesi in cui qualcuno – un testimone, l'imputato… – abbia negato di conoscere qualcun altro. Se i due si fossero chiamati, i tabulati potrebbero smentirlo; magari il contenuto delle loro telefonate è processualmente insignificante, ma il metadato non lo è,

[2] Le indicazioni al riguardo potrebbero essere sterminate. Fra i contributi italiani possiamo ricordare V. BONINI, *La nozione e le caratteristiche*, in P. MAGGIO (a cura di), *La nuova disciplina delle intercettazioni*, Torino, 2023, p. 40; S. MARCOLINI, *La* data retention *nei sistemi giuridici comunitario e italiano*, in R. FLOR, S. MARCOLINI (a cura di), *Dalla* data retention *alle indagini ad alto contenuto tecnologico*, Torino, 2022, p. 20 e 50 s. Oltreoceano è molto citata la *concurring opinion* di S. Sotomayor a United States v. Jones, 565 U.S. 400 (2012).

[3] B. TURNER, *When Big Data Meets Big Brother: Why Courts Should Apply United States v. Jones to Protect People's Data*, 16 *North Carolina Journal of Law&Technology* 377 (2015), p. 399.

perché autorizza a trarre conclusioni sulla credibilità d'un individuo. Si potrebbero fare altri esempi.

Per tutte queste ragioni, le Corti europee hanno ripetutamente segnalato che l'acquisizione dei dati di traffico non è meno lesiva dell'intercettazione[4]: trattandosi di strumenti diversi, le regole non devono per forza combaciare in ogni dettaglio, ma il livello di garanzie dev'essere omogeneo. Tuttavia queste affermazioni stentano a essere ricevute dai giudizi nazionali, che sul punto si mostrano meno sensibili[5].

2. Casi difficili

La seconda area tematica è composta dagli strumenti investigativi il cui "incasellamento" è difficoltoso. Si tratta di un'area densamente popolata, perché l'inesauribile fantasia della prassi applicativa sforna di continuo casi problematici, che cadono proprio sul confine del concetto tracciato dalle sezioni unite. Cosa succede quando un funzionario di polizia arresta in flagranza un individuo, gli sequestra il cellulare e, mentre ha l'apparecchio in mano, risponde a una chiamata, mentendo sulla sua identità o semplicemente tacendola? Non sono stati usati strumenti che potenzino le naturali capacità dei sensi, è vero[6]; però il contenuto

[4] Corte eur. dir. uomo, grande camera, sent. 23 maggio 2021, Cenrum för rättvisa c. Svezia; Corte eur. dir. uomo, grande camera, sent. 25 maggio 2021, Big brother watch c. Regno unito, spec. § 363; CGUE, grande sezione, sent. 6 ottobre 2020, causa C-623/17, Privacy international c. Secretary of State for Foreign and Commonwealth Affairs e altri; CGUE, grande sezione, sent. 6 ottobre 2020, causa C 511/18 e abbinate, La Quadrature du Net e altri c. contro Premier ministre e altri, spec. § 117 e § 184; CGUE, grande sezione, sent. 5 aprile 2022, G.D. c. The Commissioner of an Garda Síochána, spec. § 45.

[5] A dire il vero, una equiparazione alle intercettazioni era stata tentata da Cass., Sez. un., sent. 13 luglio 1998 n. 21, Gallieri, in *Giust. pen.*, 1999, III, c. 614 s., che tuttavia è stata rapidamente contraddetta dalla giurisprudenza posteriore (cfr. Cass., Sez. un., sent. 23 febbraio 2000 n. 6, D'Amuri, in *Giur. it.*, 2001, p. 1707; Cass., Sez. un., 21 giugno 2000 n. 16, Tammaro, in *Giur. it.*, 2000, p. 2122). Probabilmente i tempi non erano maturi; oggi, alla luce della giurisprudenza europea citata nella nota precedente, una presa di posizione in tal senso sarebbe più solida.

[6] Questo profilo è parso decisivo a C. Di Martino in C. DI MARTINO, T. PROCACCIANTI (a cura di), *Le intercettazioni telefoniche*, Padova, 2001, p. 18; Cass., sez. IV,

della chiamata viene appreso solo grazie a un inganno o, nella migliore delle ipotesi, a una reticenza.

Cosa succede quando il direttore d'un carcere, su richiesta d'un pubblico ministero, prende una lettera scritta o diretta a un detenuto, la apre, ne fotocopia il contenuto, imbusta nuovamente e inoltra? Lo può fare? È un'intercettazione di corrispondenza epistolare? In fondo la nozione forgiata dalle sezioni unite non limita i tipi di comunicazione suscettibili d'essere intercettate[7].

Cosa succede quando un privato, per esempio la vittima d'una estorsione, si mette d'accordo con la polizia per incontrare l'autore del reato, registrare di nascosto il colloquio e poi passare le registrazioni alla polizia? Quest'ultima figura – di solito chiamata "agente segreto attrezzato per il suono" – presenta tratti talmente peculiari che converrà fermarcisi un minuto.

Benché non manchino precedenti più remoti, possiamo partire dalla decisione con cui le sezioni unite da un lato esclusero che la manovra costituisse intercettazione (perché eseguita non da un terzo ma da uno degli interlocutori); dall'altro, ammonirono che l'espediente non poteva essere adoperato per eludere capisaldi del diritto probatorio[8]. Fra le disposizioni che la Corte di legittimità ritenne esposte a questo pericolo d'aggiramento, vale la pena ricordarne due: l'art. 63 e l'art. 195, co. 4 c.p.p. Esse restringevano molto, fin quasi ad annullare, lo spazio lasciato al

---

sent. 7 novembre 2001 n. 7724, Bregasi, in *Archivio della nuova procedura penale*, 2002, p. 271; Cass., sez. IV, sent. 25 giugno 2008, Leonardi, in *Guida dir.*, 2008, 40, p. 86; *contra*, C. SCACCIANOCE, *Approvvigionamento di flussi e dati tramite il dispositivo elettronico altrui*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, p. 39 s.

[7] Malgrado ciò, Cass., Sez. un., sent. 19 aprile 2012 n. 28997, Pasqua (in *Cass. pen.*, 2013, 955, con nota adesiva di C. RENOLDI, *Le Sezioni unite sul controllo del contenuto della corrispondenza di persona ristretta in un istituto penitenziario*) ha escluso che gli artt. 266-271 si prestino ad abbracciare la corrispondenza cartacea; nello stesso senso, L. CALÒ, *Art. 15 Cost.: quello strenuo conflitto tra garanzia e limitazione della corrispondenza*, in *Cass. pen.*, 2009, p. 628 s.; C. FANUELE, *Sequestro di corrispondenza proveniente da persona detenuta: una forma d'intercettazione "mascherata"*, in *Dir. pen. proc.*, 2010, p. 471; S. TESORIERO, *Uno strano ordine di esibizione della corrispondenza sospeso tra sequestro e intercettazione*, in *Cass. pen.*, 2008, p. 668 s.

[8] Cass., Sez. un., sent. 28 maggio 2003 n. 36747, Torcasio, in *CED Cass.*, n. 225465.

nostro metodo d'indagine: se la persona registrata di nascosto fosse quella sottoposta alle indagini, verrebbe scalzato l'art. 63; se fosse una persona informata sui fatti, verrebbe scavalcato l'art. 195, co. 4 c.p.p. (almeno qualora si volesse usare la registrazione nel dibattimento)[9]. Non per caso, uno dei massimi esperti d'intercettazioni commentò la decisione scrivendo: «le sezioni unite decretano la morte dell'agente segreto attrezzato per il suono»[10].

Ma la prognosi era clamorosamente sbagliata: l'agente segreto è vivo e gode d'ottima salute. La giurisprudenza successiva s'è infatti staccata dal precedente ed è andata componendo un panorama variopinto, nel quale si possono isolare quattro indirizzi. Secondo alcune decisioni, siccome la registrazione non è frutto d'una intercettazione, la prova è ammissibile senza limiti[11]; in sostanza, si recepisce la prima parte del ragionamento delle sezioni unite, dimenticando la seconda. Altre pronunce distinguono a seconda che l'agente segreto permetta alla polizia d'ascoltare in tempo reale oppure le ceda le registrazioni a cose fatte: il primo caso sarebbe un'intercettazione, il secondo no[12]. Altre ancora escludono sempre che si tratti d'intercettazione; tuttavia, siccome la *privacy* dell'ignaro interlocutore è pur sempre compromessa, servirebbe almeno un'autorizzazione del pubblico ministero[13]. L'ultimo indirizzo,

[9] L'art. 195, co. 4, mira a due scopi: salvaguardare il principio di separazione funzionale delle fasi, cioè la tendenziale impermeabilità del dibattimento alle risultanze conoscitive pregresse; evitare aggiramenti della disciplina sulla documentazione degli atti. Usare nelle indagini la registrazione sonora formata dall'agente segreto non urterebbe con nessuna di queste finalità.

[10] L. FILIPPI, *Le Sezioni unite decretano la morte dell'agente segreto "attrezzato per il suono"*, in *Cass. pen.*, 2004, p. 2094 s.

[11] Cass., sez. VI, sent. 24 febbraio 2009 n. 16986, Abis, in *Cass. pen.*, 2010, p. 3178; Cass., sez. VI, sent. 11 giugno 2009 n. 41799, Calciano, in *Cass. pen.*, 2010, p. 4305; Cass., sez. II, sent. 6 luglio 2022 n. 40148, Acanfora, in *CED Cass.*, n. 283977; Cass., sez. II, 21 settembre 2022 n. 46185, Puzone, in *CED Cass.*, n. 284226.

[12] Cass., sez. I, sent. 23 gennaio 2002 n. 30082, Aquino e altro, in *Riv. pen.*, 2003, p. 273; Cass. sez. II, sent. 24 febbraio 2010, in *Giur. it.*, 2011, p. 1398; Cass., sez. III, sent. 23 marzo 2016 n. 39378, C., in *Giur. it.*, 2017, p. 492.

[13] Cass., sez. VI, sent. 7 aprile 2010 n. 23742, Angelini, in *Giur. it.*, 2011, p. 183 s.; Cass., sez. II, sent. 14 ottobre 2010, Biffis, in *Foro it.*, 2011, II, c. 224 s.; Cass., sez. II,

a quanto risulta, è stato seguito solo da un giudice di merito; eppure, è molto rigoroso. Se sul piano del diritto interno la qualificazione giuridica può essere dibattuta, non si può invece mettere in discussione che l'espediente comprima il diritto al rispetto della vita privata tutelato dall'art. 8 Cedu[14]; conseguentemente, l'operazione dev'essere disposta *in accordance with the law*; e non basta una *law* qualsiasi, ne occorre una che assicuri i requisiti pretesi a Strasburgo (chiarezza, prevedibilità, determinazione dei soggetti che possono subire la misura, eccetera). Ora, osserva acutamente quel giudice: solo se s'inquadra l'operazione fra le intercettazioni questi requisiti sono soddisfatti; se la si lascia alle attività d'indagine innominate, ci si pone automaticamente fuori dalla legalità convenzionale[15].

3. Un paradosso

L'agente segreto attrezzato per il suono è una figura dai tratti quasi surreali: se ne discute da più di quarant'anni[16] e ancora non si è riusciti a mettere un punto fermo; non solo, ma una decisione presa a sezioni unite è stata rinnegata, senza che si sia sentito il bisogno d'investire nuovamente il supremo collegio, come pure vorrebbe l'art. 618, co. 1-*bis* c.p.p. Al tempo stesso, lo dicevamo, è solo la punta dell'iceberg; i casi problematici sono tanti e, visti nell'insieme, ci mettono di fronte a un paradosso: le operazioni di qualificazione giuridica a cui l'interprete

sent. 10 ottobre 2012 n. 42939, Zupo e altri, in *CED Cass.*, n. 253819; Cass., sez. IV, sent. 11 luglio 2017, in *Cass. pen.*, 2018, p. 2937.

[14] Cfr. Corte eur. dir. uomo, sent. 10 marzo 2009, Bykov c. Russia; Corte eur. dir. uomo, sent. 25 ottobre 2007, Van Vondel c. Paesi bassi; Corte eur. dir. uomo, sent. 1 marzo 2007, Heglas c. Repubblica Ceca (su questa decisione, L. DE MATTEIS, *Acquisizione di tabulati e registrazione della conversazione da parte di un interlocutore al vaglio della Corte europea dei diritti dell'uomo*, in *Cass. pen.*, 2007, p. 3947); Corte eur. dir. uomo, sent. 8 aprile 2003, M.M. c. Paesi Bassi; Corte eur. dir. uomo, sent. 5 novembre 2002, Allan c. Regno Unito; Corte eur. dir. uomo, sent. 23 novembre 1993, A. c. Francia.

[15] Trib. Lecce, 19 maggio 2008, Spagnolo, in *Cass. pen.*, 2009, p. 3088 s.

[16] Cfr. M. SCAPARONE, *Agenti segreti di polizia*, in *Riv. it. dir. e proc. pen.*, 1972, p. 146 s.

è chiamato in queste situazioni hanno una posta in gioco alta; da una parte non c'è nulla, nel nostro diritto probatorio, che goda di garanzie paragonabili a quelle previste per le intercettazioni; dall'altra, quando si conclude nel senso che un certo strumento d'indagine non sia un'intercettazione, per lo più si refluisce verso le attività investigative atipiche, per le quali la legge non appresta alcuna cautela. Insomma, la scelta è capitale: o tutto o niente; o le intercettazioni, cioè il massimo delle garanzie, oppure le attività investigative innominate, cioè l'anarchia. Una scelta con ricadute di tale peso vorrebbe termini di riferimento netti; invece, la legge non detta definizioni e quelle coniate dalla giurisprudenza lasciano irrisolti molti quesiti, consegnando così all'interprete un ambito di discrezionalità e una responsabilità senz'altro eccessivi.

4. L'innovazione tecnologica e la crisi del concetto di comunicazione: a) il "comportamento comunicativo"

Questo paradosso contrassegna da sempre la disciplina delle intercettazioni ma negli ultimi anni s'è aggravato, soprattutto per effetto dell'innovazione tecnologica, che ha agito in molte direzioni. In primo luogo, ha moltiplicato gli strumenti d'indagine la cui qualificazione giuridica è precaria: dal *thermal imager* venuto alla ribalta in un celeberrimo caso statunitense[17] all'*IMSI catcher*, anch'esso molto conosciuto all'estero ma esaminato anche in una vicenda giurisprudenziale nostrana[18].

[17] Kyllo v. United States, 533 U.S. 27 (2001). In quell'occasione la polizia sospettava che Kyllo coltivasse marijuana, e ha puntato contro la sua abitazione una "termocamera" – un apparecchio che misura il calore degli oggetti – scoprendo che due stanze erano inspiegabilmente calde: ciò autorizzava a ipotizzare che vi fossero installate lampade speciali, generalmente adoperate da chi coltiva cannabis. La Corte suprema stabilì che la polizia aveva eseguito una *search*, ma senza munirsi preventivamente del necessario mandato.

[18] Cass., sez. IV, sent. 12 giugno 2018 n. 41385, Casella, in *CED Cass.*, n. 273929. L'*IMSI catcher* è uno strumento che simula un ponte radio, in modo da indurre i cellulari nei paraggi ad agganciarsi a lui anziché ai ponti radio "veri" e carpirne il codice IMEI (che contrassegna ogni singolo cellulare) o il codice IMSI (che individua ogni

In secondo luogo, uno degli "ingredienti" del concetto d'intercettazione, ossia la "comunicazione", ha subito una serie di scossoni. Uno è stato portato dall'avvento delle videocamere: quando vengono adoperate per monitorare di nascosto condotte tenute in un domicilio, le prove raccolte possono essere utilizzate solo a patto di trovare un "ombrello" normativo che, riempiendo la riserva di legge fissata nell'art. 14 Cost., possa offrire un riparo all'attività. Sin dalla prima decisione intervenuta sul tema[19], quell'ombrello è stato trovato proprio nelle disposizioni sulle intercettazioni: la giurisprudenza ha infatti ritenuto che gli artt. 266-271 si prestino ad abbracciare non soltanto le comunicazioni verbali ma anche le condotte che comunque veicolano un messaggio, cioè i "comportamenti comunicativi"[20]. Abbiamo già criticato quest'idea in altre occasioni e non è il caso di ripetersi ora; ai fini del discorso che s'intende svolgere è importante evidenziare soltanto un profilo: il concetto di "comportamento comunicativo" è slabbrato, terribilmente incerto[21]; in una materia presidiata dal principio di legalità, dovrebbe essere un difetto; invece, alcune decisioni fanno venire il dubbio che proprio la sua ambiguità lo renda utile e ben accetto; riprenderemo l'argomento fra poco.

---

singola SIM card). Sull'argomento chi scrive ha tentato qualche riflessione in *Il cacciatore di Imsi*, in *Archivio penale*, 2020, p. 177 s.

[19] Cass., sez. VI, sent. 10 novembre 1997 n. 4397, Greco, in *Cass. pen.*, 1999, p. 1190.

[20] C. cost., sent. 24 aprile 2002, n. 135; Cass., Sez. un., sent. 28 marzo 2006 n. 26795, Prisco, in *Riv. it. dir. proc. pen.*, 2006, p. 1548.

[21] A. BALSAMO, A. TAMIETTI, *Le intercettazioni, tra garanzie formali e sostanziali*, in A. BALSAMO, R.E. KOSTORIS (a cura di), *Giurisprudenza europea e processo penale italiano*, Torino, 2008, p. 462; A. CAMON, *Captazione di immagini (diritto processuale penale)*, in *Enc. Dir., Annali*, VI, Milano, 2013, p. 143 s.; C. CONTI, *Le video-riprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi «riservati»*, in *Dir. pen. proc.*, 2006, 1361; L. CRICRÌ, voce *Videoregistrazione*, in *Enc. Giur. Treccani*, XXXII, Roma, 2006, p. 2; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007, p. 177; G. TABASCO, *Corte costituzionale e videoriprese di condotte non comunicative: ancora dubbi e perplessità*, in *Dir. pen. proc.*, 2010, p. 241; ID., *Prove non disciplinate dalla legge nel processo penale*, Napoli, 2011, p. 159.

5. Segue: b) i messaggi già arrivati

Ulteriori scossoni sono venuti dalla rivoluzione informatica, che ha esasperato un vecchio problema e ne ha fatto nascere uno nuovo. Il problema vecchio: una comunicazione resta tale anche quando ormai è giunta a destinazione o è protetta soltanto mentre viaggia? La Corte costituzionale, con una decisione molto notata e apprezzata, ha sposato la prima tesi:

> degradare la comunicazione a mero documento quando non più *in itinere*, è soluzione che, se confina in ambiti angusti la tutela costituzionale prefigurata dall'art. 15 Cost. nei casi, sempre più ridotti, di corrispondenza cartacea, finisce addirittura per azzerarla, di fatto, rispetto alle comunicazioni operate tramite posta elettronica e altri servizi di messaggistica istantanea, in cui all'invio segue immediatamente – o, comunque sia, senza uno iato temporale apprezzabile – la ricezione[22].

Il quesito, dunque, ormai è risolto; malgrado ciò, è interessante guardare come la giurisprudenza aveva ragionato fino alla decisione della Consulta. In sostanza la Corte di Cassazione aveva spezzato in due il concetto di comunicazione a seconda che esso operasse sul terreno del diritto sostanziale oppure del diritto processuale[23]. Quando si trattava di punire i delitti contro l'inviolabilità dei segreti, le nozioni di «comunicazione» e «corrispondenza» venivano allargate ai messaggi

[22] C. cost., sent. 27 luglio 2023 n. 170, in *Giur. cost.*, 2023, p. 1713 ss.

Come osserva P. VILLASCHI (*La posta elettronica e i messaggi WhatsApp sono corrispondenza? Note a margine del ricorso per conflitto di attribuzione tra poteri dello Stato promosso dal Senato della Repubblica in relazione al "caso Renzi"*, in *federalismi.it* (rivista web), 2023, 7, p. 247 ss., ultimo accesso il 28 febbraio 2025), che questa fosse l'opinione della Consulta poteva essere desunto già da C. cost., sent. 11 marzo 1993 n. 81, secondo la quale l'acquisizione, presso i fornitori del servizio, dei tabulati del traffico telefonico è attività regolata dall'art. 15 Cost.: in questi casi, infatti, si tratta proprio di controllare gli estremi di comunicazioni già svolte.

[23] Lo notano M. BORGOBELLO, *Il concetto di "corrispondenza" nella sentenza 170 del 2023 della Corte costituzionale*, in *Giurisprudenza penale*, 2023, 7/8, p. 9; P. VILLASCHI, *La posta elettronica*, cit., p. 348 s.

già ricevuti[24]. Quando invece si trattava di raccogliere prove, allora s'è detto che sms, *WhatsApp*, messaggi di posta elettronica scaricati e conservati nella memoria d'un apparecchio non sono comunicazioni ma documenti (art. 234 c.p.p.), cosicché la loro acquisizione non soggiace né alle regole stabilite per la corrispondenza né alla disciplina delle intercettazioni[25]. Gli stessi principi sono stati applicati alla corrispondenza cartacea[26]. Vale la pena portare alla luce un dettaglio: l'unico caso in cui la Corte di Cassazione ha applicato le norme sulle intercettazioni all'acquisizione di e-mail già ricevute è un caso nel quale il decreto di au-

[24] «Integra il reato di violazione, sottrazione e soppressione di corrispondenza (art. 616 c.p.) […] la condotta di colui che prende cognizione del contenuto della corrispondenza telematica intercorsa tra la ex convivente e un terzo soggetto, conservata nell'archivio di posta elettronica della prima»: Cass., sez. V, sent. 2 gennaio 2017 n. 12603, Segagni e altro, in *CED Cass.*, n. 269517 – 01.

In effetti la sistematica dei delitti contro l'inviolabilità dei segreti fornisce spunti che possono essere valorizzati in questa direzione. L'art. 616 c.p. punisce chi «prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta», mentre gli artt. 617 e 617-*quater* c.p. incriminano chi «fraudolentemente, prende cognizione» o «intercetta» comunicazioni; per distinguere la prima fattispecie dalle altre due si potrebbe far leva sulla natura fraudolenta della condotta, richiesta soltanto dalle disposizioni del secondo gruppo; ma si può anche ritenere che «mentre l'art. 617-*quater* c.p. […] riferisce il termine "corrispondenza" alla comunicazione nel suo momento dinamico, ossia in fase di trasmissione, l'art. 616 c.p. […] tipizza le condotte riferite alla comunicazione dal punto di vista statico, cioè il pensiero già comunicato»: così Cass., sez. V, sent. 29 settembre 2020 n. 30735, in *Dejure*; analogamente, Cass., sez. V, sent. 2 gennaio 2017 n. 12603, Segagni e altro, in *CED Cass.*, n. 269517 – 01; in dottrina, R. Rinaldi, in R. RINALDI, L. PICOTTI (a cura di), *Art. 6 l. 23 dicembre 1993, n. 547*, in *Leg. pen.*, 1996, p. 119 s. Dal canto loro, gli artt. 617 e 617-*quater* c.p. puniscono anche la rivelazione delle comunicazioni telefoniche o telegrafiche intercettate o di cui s'è presa cognizione, e la rivelazione, nella normalità dei casi, avviene *ex post*, cioè quando la trasmissione del messaggio c'è già stata.

[25] Cass., sez. III, sent. 25 novembre 2015 n. 928, Giorgi, in *CED Cass.*, n. 265991 – 01; Cass., sez. V, sent. 21 novembre 2017, *ivi*, n. 272319 – 01; Cass., sez.VI, sent. 28 maggio 2019 n. 28269, Pizzarotti, *ivi*, n. 276227 – 01; Cass., sez. III, sent. 16 aprile 2019 n. 29426, Moliterno, *ivi*, 276358 – 01; Cass., sez. VI, sent. 12 novembre 2019 n. 1822, Tacchi, *ivi*, 278124 – 01; Cass., sez. VI, sent. 6 febbraio 2020 n. 12975, Ceriani, *ivi*, n. 278808 – 02; Cass., sez. VI, sent. 16 marzo 2022 n. 22417, Sgromo, *ivi*, n. 283319 – 01.

[26] Cass., sez. I, sent. 23 aprile 2014 n. 24919, Attanasio, in *CED Cass.*, n. 262303 – 01.

torizzazione del giudice per le indagini preliminari effettivamente c'era; perciò, estendere le norme sulle intercettazioni era gratis, cioè non metteva a rischio le conoscenze raccolte[27].

6. Segue: c) gli scambi fra macchine

Veniamo al problema nuovo. Prima della rivoluzione digitale s'insegnava che

> la corrispondenza, nel senso della nostra legge penale, […] abbraccia […] quei rapporti psichici diretti, ancorché mediati, i quali consistono nella *comunicazione* di idee, di sentimenti, di propositi o di notizie, *che una persona fa direttamente a una o più altre persone determinate*[28].

Le cose erano destinate a ingarbugliarsi in seguito alla legge sui reati informatici. Il legislatore voleva lasciarsi alle spalle il concetto di comunicazione come scambio fra individui; la relazione al disegno di legge destinato a sfociare nella l. 23 dicembre 1993 n. 547 lo spiega chiaramente, descrivendo una manovra normativa portata avanti su due fronti: sul versante sostanziale, le fattispecie incriminatrici poste a presidio dell'inviolabilità dei segreti vengono allargate per porre rimedio al fatto che, fino a quel momento, «le norme penali disponibili (art. 617 ss. c.p.) riguarda[va]no comunicazioni tra persone e non tra persone e macchine o tra macchine»; sul versante processuale, il campo applicativo delle intercettazioni viene a sua volta ingrandito (art. 266-*bis* c.p.p.), «in simmetria e congiuntamente con la proposta rivisitazione delle fatti-

[27] Cass., sez. IV, sent. 28 giugno 2016 n. 40903, Grassi e altri, in *CED Cass.*, n. 268228 – 01. Per la precisione, nel senso dell'applicabilità degli artt. 266 e seguenti c.p.p. all'acquisizione di chat si era espressa anche Cass., sez. III, sent. 10 novembre 2015 n. 50452, Guarnera e altri, in *CED Cass.*, n. 265615 – 01, dove però non risulta chiaro se si trattasse di una acquisizione contestuale o successiva alla comunicazione; anche in quel caso, comunque, il decreto autorizzativo dell'intercettazione c'era.

[28] V. MANZINI, *Trattato di diritto penale italiano*, V edizione aggiornata da P. Nuvolone, G.D. Pisapia, VIII, a cura di G.D. Pisapia, Torino, 1985, p. 915; il corsivo è aggiunto.

specie sostanziali»[29]. Ad onor del vero, gli sviluppi successivi e il dedalo di questioni portate dai nuovi strumenti investigativi ad alto tasso tecnologico mostreranno come il legislatore, con ogni probabilità, non avesse valutato a fondo le implicazioni di questa linea di riforma; ad ogni modo, gli obiettivi erano chiari.

Sennonché, in entrambi gli ambiti, sostanziale e processuale, l'intendimento viene portato avanti in modo maldestro: sul piano sostanziale, fattispecie incriminatrici verbose, pletoriche, il cui campo d'applicazione si sovrappone di continuo[30]; sul piano processuale, una formula sibillina: dopo il 1993, l'intercettazione abbraccia anche «il flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente fra più sistemi» (art. 266-*bis* c.p.p.). La scadente fattura del prodotto legislativo lascia discrezionalità agli interpreti, e la giurisprudenza la esercita spaccando quel disegno normativo unitario che puntava a introdurre un nuovo e ampio concetto di comunicazione, valido sia sul piano sostanziale sia su quello processuale e comprensivo delle interazioni fra macchine: sul piano sostanziale, la Corte di Cassazione si mostrerà sostanzialmente allineata al legislatore; su quello processuale, invece, gli atteggiamenti saranno ondivaghi, a seconda degli obiettivi di volta in volta perseguiti.

Così, si afferma che sistemare presso sportelli bancomat apparecchiature – di solito, scanner chiamati "skimmer", per lo più accoppati a videocamere o fotocamere – capaci di carpire i dati riportati sulle carte di credito e sulle tessere bancomat nonché i relativi codici pin, integra la condotta punita dall'art. 617-*quinquies* c.p., cioè una «installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche»[31]; il "dialogo"

[29] Relazione al disegno di legge presentato dal ministro di grazia e giustizia al Senato il 26 marzo 1993 e successivamente trasferito alla Camera dei deputati l'11 giugno 1999, in *www.penale.it*.

[30] Cfr. L. PICOTTI, *Art. 5 l. 23 dicembre 1993, n. 547*, in *Leg. pen.*, 1996, p. 108 s.; ID., in R. RINALDI, L. PICOTTI, *Art. 6 l. 23 dicembre 1993, n. 547*, *ibidem*, p. 121 s.; ID., *Art. 8 l. 23 dicembre 1993, n. 547*, *ibidem*, p. 130 s.

[31] Cass., sez. V, sent. 23 gennaio 2023 n. 17814, in *Dejure*; Cass., sez. V, sent. 11 marzo 2019 n. 15665, *ibidem* (ma massimata in termini non corretti); Cass., sez. V, sent. 9 luglio 2010 n. 36601, *ibidem*; Cass., sez. II, sent. 9 novembre 2007 n. 45207, *ibidem*; Cass., sez. V, sent. 5 dicembre 2006 n. 3252, *ibidem*; App. Roma, 24 gennaio

intercettato, in tal caso, intercorre appunto fra un uomo e un dispositivo elettronico[32].

Quando ci si sposta nel processo, le cose diventano meno chiare. Consideriamo la localizzazione satellitare (a esempio attraverso il sistema GPS) degli spostamenti d'un soggetto. Come ormai abbiamo imparato, si svolge installando di nascosto su un'auto un apparecchio che registra i segnali mandati a terra dai satelliti: è un'intercettazione? No, risponde la Corte di Cassazione, perché «è […] evidente che il concetto di intercettazione […] è relativo a una attività di ascolto (o lettura) e captazione di *comunicazioni tra due o più persone*»[33].

2018, n. 255, *ibidem*; Trib. Napoli, 10 maggio 2012, *ibidem*; G.i.p. Trib. Milano, 19 febbraio 2007, *ibidem*.

[32] Cass., sez. V, sent. 5 dicembre 2006 n. 3252, in *Dejure*, parla di «utenti che comunicano con il sistema Postamat».

[33] Cass., sez. V, sent. 27 febbraio 2002 n. 16130, Bresciani e altri, in *Foro it.*, 2002, II, c. 635, con nota adesiva di A. SCAGLIONE. Lo stesso vale sul piano costituzionale: la localizzazione satellitare non richiede un'autorizzazione del magistrato perché l'art. 15 Cost. «tutela le comunicazioni interpersonali» (Cass., sez. IV, sent. 29 gennaio 2007 n. 8871, Navarro Mongort, in *CED Cass.*, n. 236112 – 01).

Dal canto suo, la dottrina è divisa sulla possibilità di considerare "comunicazione" il segnale lanciato dai satelliti che compongono il sistema GPS. Alcuni ritengono che il termine comprenda soltanto le comunicazioni *tra individui* (L. ALGERI, *Lo* Screenshot *eseguito (senza garanzie?) dal* Trojan *di Stato*, in *Giur. it.*, 2022, p. 2785; T. BENE, *Il pedinamento elettronico: truismi e problemi spinosi*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, p. 350; G. DI PAOLO, *"Tecnologie del controllo" e prova penale*, Padova, 2008, p. 255; A. PROCACCINO, *Piccoli equivoci senza importanza: tra intercettazioni di flussi informatici, perquisizioni e prove atipiche*, in *Cass. pen.*, 2022, p. 3122; S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. e proc. pen.*, 2012, p. 583; ID., *Le indagini digitali*, Torino, 2018, p. 287; E. TOMA, *Sulla configurabilità di "comportamenti comunicativi virtuali"*, in *Dir. pen. proc.*, 2022, p. 1437). Altri premono per rileggere in chiave moderna quella nozione (O. BRUNO, *La "localizzazione" elettronica tra indagine e prova*, in *Giust. pen.*, 2011, III, c. 691 e 697; P. PERETOLI, *Controllo satellitare con GPS: pedinamento o intercettazione?*, in *Dir. pen. proc.*, 2003, p. 96), che finirebbe così per abbracciare, eventualmente all'esito d'un procedimento analogico (L.G. VELANI, *Nuove tecnologie e prova penale: il sistema d'individuazione satellitare g.p.s.*, in *Giur. it.*, 2003, p. 2375), «ogni flusso di bit» (così D. IACOBACCI, *Sulla necessità di riformare la disciplina delle intercettazioni prendendo le mosse dalle esitazioni applicative già note*, in *Giust. pen.*, 2011, II, c. 365).

Ancor più significative due pronunce sul captatore informatico. La prima (caso Virruso) riguarda un procedimento in cui il *trojan* viene inserito nel computer d'ufficio d'un pubblico funzionario, per estrapolare i dati e i files già formati e contenuti nella memoria del computer, nonché quelli che in futuro vi sarebbero stati inseriti; la Corte di Cassazione esclude che si tratti di una captazione informatica, perché il concetto d'intercettazione «richiede […] un dialogo con altri soggetti»[34].

Dieci anni dopo, come in un gioco di prestigio, le conclusioni vengono capovolte. Caso Romeo: il procedimento riguarda una rete di società cartiere finalizzata all'evasione dell'IVA; interessa un file *excel* in cui l'imputato annota operazioni contabili sospette; viene acquisito con un *trojan*, e stavolta la Corte di Cassazione inquadra l'operazione fra le intercettazioni: infatti il bersaglio di questa «captazione di flussi di dati in fieri, cristallizzati nel momento stesso della loro formazione», «pur non costituendo una "comunicazione" in senso stretto, costituisce certamente […] un comportamento c.d. comunicativo, del quale è ammessa la captazione»[35]. Come gli amori di Antonello Venditti, anche certe nozioni giuridiche «fanno giri immensi e poi ritornano»: il "comportamento comunicativo", nato venticinque anni prima per legittimare le riprese visive eseguite di nascosto all'interno d'un domicilio[36], riappare qui, utile per sostenere che l'imputato che compila un file *excel*, anche se non lo manda a nessuno, comunque sta comunicando e quindi può essere legittimamente intercettato.

Si noti: sul piano concettuale, i casi Virruso e Romeo sono identici. Quel che li distingue sono le circostanze concrete: nella vicenda Virruso non c'era un decreto che autorizzasse l'intercettazione; la Corte risponde che non serviva, perché non era stata fatta un'intercettazione. Nella vicenda Romeo il decreto autorizzativo c'era; quel che mancava, semmai, era l'osservanza delle cautele che garantiscono l'integrità della prova digitale; la Corte risponde che non serviva, perché era stata fatta un'intercettazione.

---

[34] Cass., sez. V, sent. 14 ottobre 2009 n. n. 16556/2010, Virruso, in *CED Cass.*, n. 246954 – 01.

[35] Cass., sez. I, sent. 7 ottobre 2021 n. 3591/2022, Romeo, in *CED Cass.*, n. 282495 – 01.

[36] *Supra*, nt. 19.

7. Uno sguardo di sintesi sugli indirizzi della magistratura e sulle sue ideologie

Le posizioni della giurisprudenza, considerate una a una, sarebbero sostenibili, il tessuto normativo è talmente sfrangiato da consentirle. Per di più, in alcuni casi si potrebbe arrivare alle stesse conclusioni anche sulla base d'altri argomenti[37]. È piuttosto il quadro d'insieme a risultare inquietante. La nostra magistratura adopera il concetto di comunicazione come una fisarmonica il cui mantice si gonfia o si rimpicciolisce a seconda degli obiettivi di volta in volta presi di mira. Si tratta d'incriminare e di punire? Il concetto s'allarga e comprende i messaggi già giunti a destinazione[38] e quelli che intercorrono fra un uomo e una macchina[39]. Si tratta di accordare garanzie all'imputato? Il concetto si restringe e non comprende più né i messaggi ormai arrivati[40] né quelli tra macchine[41] né quelli tra uomo e macchina[42]. Si tratta di salvare una prova raccolta nell'indagine? Il concetto s'allarga di nuovo e di nuovo comprende quegli stessi scambi tra uomo e macchina che un attimo prima erano stati esclusi[43].

---

[37] Si consideri la localizzazione svolta sfruttando il sistema GPS; come dicevamo, di solito viene effettuata collocando un ricevitore nell'autovettura del soggetto da controllare; il dispositivo capta i segnali inviati dai satelliti e, triangolandoli, elabora la propria posizione e la trasmette alle forze di polizia (cfr. A. TESSITORE, C. MARINO, *Intercettazioni elettroniche e informatiche. Le tecniche*, Albino (BG), 2011, p. 7 s.). Ora, i segnali lanciati dai satelliti non sono schermati ma liberamente ricevibili (infatti sono ricevuti da chiunque adoperi un navigatore satellitare): anche a ritenere che si tratti d'una comunicazione, non si tratterebbe però d'una comunicazione *riservata* e difetterebbe dunque un requisito del concetto d'intercettazione; in tal senso, T. BENE, *Il pedinamento elettronico*, cit., p. 350; A.P. CASATI, *Le intercettazioni*, Milano, 2023, p. 21; C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007, p. 239; S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. e proc. pen.*, 2012, p. 583; M. STRAMAGLIA, *Il pedinamento satellitare: ricerca e uso di una prova "atipica"*, in *Dir. pen. proc.*, 2011, p. 214.

[38] *Supra*, nt. 24.

[39] *Supra*, nt. 32 e 33.

[40] *Supra*, nt. 25 e 26.

[41] *Supra*, nt. 34.

[42] *Supra*, nt. 35.

[43] *Supra*, nt. 36.

Non possiamo sorprendercene troppo, perché non è un atteggiamento inedito: la stessa cosa è stata fatta per il domicilio. Come hanno riconosciuto le sezioni unite in un passo di grande sincerità,

> la giurisprudenza tende ad ampliare il concetto di domicilio in funzione della tutela penale degli artt. 614 e 615-*bis* c.p., mentre tende a circoscriverlo quando l'ambito domiciliare rappresenta un limite allo svolgimento delle indagini[44].

8. Prospettive

Non tutti, ma alcuni dei problemi discussi finora sono stati visti dal legislatore, che sta cercando soluzioni, in particolare per quanto riguarda il controllo di comunicazioni ormai arrivate a destinazione. Applicare le garanzie delle intercettazioni a messaggi già trasmessi e ricevuti avrebbe un inconveniente e un pregio. L'inconveniente: difendersi dai controlli effettuati in tempo reale è molto più difficile, ed è per questo che per tali controlli s'avverte il bisogno d'una normativa rigorosa. Pensiamo ai dati di traffico: per prenderli dalle imprese che forniscono servizi di telecomunicazione serve un provvedimento del giudice; per prenderli direttamente dal telefono, basta un decreto di sequestro del pubblico ministero. Disparità irragionevole? No, perché nel primo caso l'interessato è inerme, nel secondo può proteggersi da solo, gli basta cancellare il registro delle chiamate. Il pregio: i programmi di posta elettronica e le *app* di messaggistica hanno una capacità d'archiviazione smisurata, che arriva a comprendere anni o persino decenni di messaggi; lasciare poche tutele non sarebbe equo.

Il legislatore si mostra sensibile al secondo argomento. Una proposta di legge già approvata dal Senato e attualmente all'esame della Camera prevede che, quando si sequestra un dispositivo elettronico e al suo interno si trovano comunicazioni, la loro acquisizione possa avvenire solo in presenza dei presupposti e secondo le procedure previste per l'inter-

[44] Cass., Sez. un., sent. 28 marzo 2006 n. 26795, Prisco, in *Riv. it. dir. proc. pen.*, 2006, p. 1548.

cettazione[45]. È una linea di *realpolitik*: il legislatore non s'avventura in complicate rifondazioni dogmatiche e tiene fermo il concetto tradizionale d'intercettazione come operazione condotta in tempo reale; al tempo stesso, ne sterilizza i difetti, stabilendo che i controlli postumi, quantunque non siano intercettazioni, godano di garanzie equivalenti.

L'idea è apprezzabile; il suo limite, semmai, è quello di ragionare "soltanto" sulle comunicazioni. Immaginiamo che la proposta di legge venisse definitivamente approvata e ipotizziamo un'indagine su una vicenda di pedofilia: per prendere dal cellulare del pedofilo i messaggi *WhatsApp* scambiati con la vittima, un giudice dovrebbe accertare i presupposti richiesti dagli artt. 266 e 267; per prendere il video pornografico che il pedofilo ha girato con la vittima, quei requisiti non servirebbero, perché il video non è una comunicazione. Qualcosa non torna: l'atto più invasivo sarebbe garantito meno.

Di fronte a queste storture, c'è da chiedersi se non sia giunto il momento di superare il concetto di comunicazione e i difficilissimi problemi interpretativi che esso porta con sé, per andare alla ricerca d'una nozione nuova, più ampia, capace di tutelare situazioni egualmente meritevoli di protezione. Certo, non sarebbe un compito facile.

[45] Proposta di legge d'iniziativa dei senatori Zanettin e Bongiorno, approvata dal Senato il 20 aprile 2024, trasmessa alla Camera l'11 aprile 2024 (atto camera n. 1822), art. 1.

I DATI ESTERNI DELLE COMUNICAZIONI: TENDENZE EVOLUTIVE

Federica Iovene

SOMMARIO: *1. L'evoluzione della giurisprudenza della Corte di giustizia dell'Unione europea in materia di conservazione e acquisizione dei tabulati telefonici e telematici. 2. Art. 132 d.lgs. 196/2003 (codice* privacy*) e art. 24 l. 167/2017. 3. Compatibilità con la disciplina europea: il rinvio pregiudiziale del giudice per le indagini preliminari di Bolzano. 4. La questione (irrisolta) della conservazione dei dati di traffico telefonico e telematico. 5. Riflessione: il ruolo del pubblico ministero alla luce del diritto europeo.*

1. L'evoluzione della giurisprudenza della Corte di giustizia dell'Unione europea in materia di conservazione e acquisizione dei tabulati telefonici e telematici

La disciplina italiana della conservazione e acquisizione dei c.d. tabulati telefonici e telematici è fortemente influenzata dall'evoluzione giurisprudenziale della Corte di giustizia dell'Unione europea. Le sentenze della Corte di Lussemburgo in materia si inseriscono in un contesto di sempre maggiore sensibilità a livello europeo rispetto alle sfide che le innovazioni tecnologiche pongono rispetto alla tutela dei diritti fondamentali. Infatti, nelle decisioni traspare la consapevolezza che anche forme di indagine tecnologicamente avanzata, apparentemente meno invasive della vita privata e della libertà e segretezza delle comunicazioni rispetto alle classiche intercettazioni, possano in realtà rivelarsi insidiose e permettere di acquisire informazioni sulla vita delle persone che queste ultime intendono mantenere riservate, inducendole a cambiare le proprie abitudini di vita.

Inoltre, con specifico riferimento al tema che ci interessa, la giurisprudenza europea mostra una particolare sensibilità circa il rischio di abusi e accessi illeciti a dati conservati non da soggetti pubblici, ma da

privati che inevitabilmente agiscono secondo logiche di mercato e di risparmio di spesa.

Fin dalle prime sentenze che si sono occupate di questa materia, la Corte di giustizia si è concentrata su due aspetti nodali: da un lato la fase della conservazione dei dati, dall'altro l'individuazione dell'autorità competente ad acquisire tali dati per il successivo utilizzo nell'ambito di un procedimento penale e la delimitazione dei reati per l'accertamento dei quali tale acquisizione è possibile. Il parametro a cui la Corte di Lussemburgo si è sempre ispirata nel verificare di volta in volta la compatibilità con il diritto europeo, dapprima della direttiva sulla c.d. *data retention*[1] e poi delle singole legislazioni nazionali, è sempre stato quello di valutare se l'ingerenza, che attraverso la conservazione e l'acquisizione dei tabulati viene a determinarsi nel diritto al rispetto della vita privata, sia proporzionata rispetto all'obiettivo da perseguire.

In questo filone giurisprudenziale, la prima pronuncia da ricordare è la sentenza dell'8 aprile 2014, *Digital Rights*[2]. Con tale decisione la Corte di giustizia, chiamata a verificare la compatibilità con il diritto dell'Unione della direttiva *data retention*, ne ha sancito l'invalidità a seguito di un rigoroso vaglio di proporzionalità tra obiettivo perseguito e diritti fondamentali coinvolti.

In particolare, la Corte di Lussemburgo ha dichiarato invalida la direttiva *data retention*, tra l'altro: (1) perché prevedeva la conservazione indiscriminata dei dati delle comunicazioni di qualsiasi persona, a prescindere da qualsivoglia collegamento con reati gravi, e non limitava la conservazione a un determinato periodo di tempo, a una zona geografica o a una cerchia di persone che potessero essere coinvolte in un reato grave; (2) perché non prevedeva che l'acquisizione dei dati avvenisse con provvedimento di un giudice o di un'autorità amministrativa indipendente e solo nell'ambito di indagini riguardanti forme di criminalità grave.

[1] Direttiva 2006/24/CE del Parlamento e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.

[2] CGUE, grande sezione, sent. 8 aprile 2014, cause C-293/12 e C-594/12, Digital Rights Ireland Ltd.

Già per effetto di tale sentenza la disciplina dell'art. 132 codice *privacy*, che era stata modificata proprio in base alle disposizioni della direttiva *data retention*, doveva ritenersi incompatibile con il diritto dell'Unione europea e, in forza della primazia e dell'effetto diretto di quest'ultimo, andava disapplicata in quanto non conforme ai principi espressi dalla Corte di giustizia[3].

Tuttavia, dopo che i medesimi principi sono stati ribaditi dalla Corte di Lussemburgo nelle sentenze del 21 dicembre 2016, *Tele 2*[4], e del 6 ottobre 2020, *La Quadrature du Net*[5], si è dovuto attendere la sentenza del 2 marzo 2021, Prokuratuur[6] per comprenderne la portata e gli effetti sul diritto nazionale.

In quest'ultima decisione, che ha costituito poi la base per ulteriori modifiche all'art. 132 codice *privacy*, il rinvio pregiudiziale investiva direttamente la compatibilità con il diritto europeo, e in particolare con l'art. 15 § 1 della direttiva 2002/58/CE[7] e con i diritti fondamentali sanciti dagli articoli 7, 8 e 11 Carta dir. fond. UE, di una legislazione nazionale – in particolare di quella della Romania – in materia di conservazione dei tabulati.

Le risposte della Corte di giustizia non cambiano. Così come la direttiva *data retention* era incompatibile con il diritto dell'Unione, perché prevedeva obblighi di conservazione generalizzati e indifferenziati

[3] Sul punto sia consentito rinviare a F. IOVENE, Data retention *tra passato e futuro. Ma quale presente?*, in *Cass. pen.*, 2014, p. 4274; si veda altresì R. FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d.* "data retention" *contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Diritto penale contemporaneo - Rivista trimestrale*, 2014, 2, p. 178.

[4] CGUE, grande sezione, sent. 21 dicembre 2016, cause C203/15 e C689/15, Tele2 Sverige AB.

[5] CGUE, grande sezione, sent. 6 ottobre 2020, cause C-511/18, C-512/18 e C-520/18, La Quadrature du Net e altri.

[6] CGUE, grande sezione, sent. 2 marzo 2021, causa C-746/18, H.K. con l'intervento di Prokuratuur. Per un commento alla sentenza si veda P. DI 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, p. 2563.

[7] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

e non prevedeva che l'accesso ai dati conservati fosse possibile solo per il perseguimento di forme gravi di criminalità e con provvedimento di un giudice o di un'autorità amministrativa indipendente, allo stesso modo con la sentenza del 2 marzo 2021 la Corte di Lussemburgo ha ritenuto come il diritto europeo osti a una normativa nazionale che non circoscriva l'accesso ai dati conservati solo in relazione a necessità di accertamento di reati gravi e con provvedimento del giudice o di un'autorità amministrativa indipendente.

Con la sentenza Prokuratuur la Corte di giustizia ha inoltre ribadito che l'acquisizione dei tabulati può avvenire solo per mano di un soggetto terzo rispetto alle parti di un procedimento penale. Ne consegue che il pubblico ministero, che non è terzo rispetto al processo penale, non può essere l'autorità competente a disporre l'acquisizione dei tabulati telefonici e telematici.

Per effetto di questa pronuncia, l'art. 132 codice *privacy* è stato modificato dal d.l. 30 settembre 2021 n. 132, convertito con modificazioni nella l. 23 novembre 2021 n. 178 (su cui v. *infra*).

La Corte di giustizia è poi tornata a pronunciarsi in merito alla disciplina relativa all'acquisizione dei tabulati nella sentenza del 5 aprile 2022[8].

In questa sentenza la Corte di Lussemburgo si è concentrata sul profilo della conservazione dei dati. In particolare, essa ha sviluppato, esplicitandone le conseguenze sul piano degli effetti negli ordinamenti nazionali, il tema della distinzione tra conservazione dei dati e accesso ai dati, chiarendo che si tratta di due aspetti distinti che comportano entrambi gravi ingerenze nel diritto alla vita privata e alla libertà di espressione, richiedendo autonome giustificazioni. È stato così riaffermato il principio secondo cui il diritto dell'Unione osta a una normativa nazionale che preveda una conservazione generalizzata e indifferenziata dei dati di traffico e relativi all'ubicazione, con la finalità di lotta contro gravi forme di criminalità e di prevenzione di minacce gravi alla sicurezza pubblica.

Pertanto, una disciplina nazionale – come quella italiana nella formulazione attuale – che garantisca il pieno rispetto delle condizioni ri-

[8] CGUE, grande sezione sent. 5 aprile 2022, causa C-140/20, G.D.

sultanti dalla giurisprudenza che ha interpretato la direttiva 2002/58/CE in materia di accesso ai dati conservati, ossia la sentenza *Prokuratuur* del 2 marzo 2021, non può – per sua natura – essere idonea né a limitare e neppure a rimediare alla grave ingerenza che conseguirebbe dalla conservazione indiscriminata di tali dati.

Le ingerenze nel diritto al rispetto della vita privata determinate dalla conservazione e dall'acquisizione sono da trattare distintamente e, quindi, la normativa nazionale deve rispettare i principi espressi dalla Corte di Lussemburgo con riferimento ai presupposti e ai limiti di ciascuna forma di ingerenza in tale diritto fondamentale.

Infatti, secondo la giurisprudenza consolidata della Corte di giustizia, affinché la disciplina nazionale avente ad oggetto la conservazione e l'acquisizione dei tabulati telefonici e telematici, sia compatibile con il diritto europeo e in particolare con l'art. 15 § 1 della direttiva 2002/58/CE e con i diritti fondamentali sanciti dagli articoli 7, 8 e 11 Carta dir. fond. UE, occorre:

1. che la conservazione dei dati c.d. esterni di traffico telefonico e telematico non sia generalizzata e indiscriminata, ma sia delimitata sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico;
2. che l'acquisizione avvenga con provvedimento di un'autorità terza e indipendente e sia giustificata dalla necessità di perseguire forme gravi di criminalità.

Bisogna a questo punto domandarsi quali siano le conseguenze per una disciplina nazionale che non rispetti questi principi e sia quindi incompatibile con il diritto dell'Unione.

Come ci ricorda la stessa Corte di giustizia nella sentenza del 5 aprile 2022, il principio della *primauté* del diritto dell'Unione europea impone a tutte le istituzioni degli Stati membri di dare piena efficacia alle varie disposizioni del diritto europeo e, quindi – ove non sia possibile procedere a un'interpretazione conforme del diritto nazionale – il giudice nazionale deve disapplicare la norma interna in contrasto con il diritto europeo, senza doverne chiedere o attendere la rimozione in via legislativa o mediante altro procedimento costituzionale. L'effetto della disapplicazione, ricorda la Corte, non può che essere retroattivo, salva la possibilità, solo da parte sua e solo in via eccezionale, di prevedere

nella sentenza una limitazione nel tempo degli effetti della pronuncia interpretativa; infatti,

> il primato e l'applicazione uniforme del diritto dell'Unione risulterebbero pregiudicati se i giudici nazionali avessero il potere di attribuire alle norme nazionali, anche solo provvisoriamente, il primato rispetto al diritto dell'Unione al qual esse contravvengono[9].

Fatta questa doverosa premessa sulla giurisprudenza della Corte di giustizia, va ora brevemente ripercorsa l'evoluzione normativa della disciplina italiana sulla conservazione e acquisizione dei tabulati telefonici per verificare se la stessa, a seguito dell'ultima novella, sia compatibile con il diritto dell'Unione, affrontando i due diversi aspetti della conservazione e dell'acquisizione dei dati di traffico telefonico e telematico.

2. Art. 132 d.lgs. 196/2003 (codice privacy*) e art. 24 l. 167/2017*

La disciplina relativa alla conservazione e acquisizione dei dati di traffico e relativi all'ubicazione per finalità di accertamento e persecuzione dei reati nel nostro ordinamento è contenuta nell'art. 132 d.lgs. 30 giugno 2003 n. 196, c.d. codice *privacy*, e nell'art. 24 l. 20 novembre 2017 n. 167 per i reati di cui agli artt. 51, co. 3-*quater* e 407, co. 2 lett. a) c.p.p.

L'art. 132 codice *privacy*, introdotto nella sua versione originaria nel 2003 e più volte modificato, interveniva con la finalità di dettare una disciplina positiva di questo strumento di ricerca della prova, i cui presupposti erano stati elaborati fino a quel momento solo in via giurisprudenziale, attraverso il confronto con la disciplina delle intercettazioni e muovendo dall'assunto che l'acquisizione dei tabulati incidesse sul diritto alla segretezza delle comunicazioni in misura inferiore rispetto alle prime e che, pertanto, fosse sufficiente quel "livello minimo di garanzie" costituito dal decreto motivato del pubblico ministero.

[9] CGUE, grande sezione sent. 5 aprile 2022, causa C-140/20, G.D., § 119.

La Corte costituzionale, con la sentenza n. 81 del 1993[10] aveva gettato le basi per il corretto inquadramento di tale mezzo di ricerca della prova sul piano delle garanzie costituzionali, affermando che si trattava di un istituto diverso da quello delle intercettazioni, ma che comunque ricadeva nell'area di tutela dell'art. 15 Cost. e che, pertanto, occorreva quel «livello minimo di garanzie costituito dal provvedimento motivato dell'autorità giudiziaria». Con la sentenza n. 281 del 1998[11] la Corte costituzionale è tornata a pronunciarsi sul tema riconoscendo che quel "livello minimo di garanzie" era rispettato laddove i tabulati venissero acquisiti con decreto motivato del pubblico ministero in base all'art. 256 c.p.p.

Sono poi intervenute le sezioni unite della Corte di Cassazione che, a più riprese, hanno confermato che, per l'acquisizione dei tabulati, era sufficiente il decreto motivato del pubblico ministero, in ragione del minor grado di lesività della segretezza delle comunicazioni rispetto a quello determinato dalle intercettazioni[12].

L'art. 132 codice *privacy*, nella parte relativa alla durata della conservazione dei dati, è stato modificato da ultimo dal d.lgs. 30 maggio 2008 n. 109[13] di attuazione della direttiva *data retention* con finalità di armonizzazione della disciplina dei tabulati all'interno dell'Unione europea e prevede che i dati di traffico, compresi quelli relativi all'ubicazione, vengano conservati dal fornitore per finalità di accertamento e repressione dei reati per ventiquattro mesi nel caso dei dati di traffico telefonico, dodici mesi nel caso dei dati di traffico telematico e trenta giorni nel caso dei dati relativi alle chiamate senza risposta.

L'art. 24 l. 20 novembre 2017 n. 167 prevede per i reati di cui agli artt. 51, co. 3-*quater* e 407, co. 2 lett. a) c.p.p. l'obbligo di conservazione di dati di traffico telefonico, telematico e relativo alle chiamate sen-

[10] C. cost., sent. 11 marzo 1993 n. 81.

[11] C. cost., sent. 17 luglio 1998 n. 281.

[12] Cass., sez. un., sent. 23 febbraio 2000 n. 6, D'Amuri, in *CED Cass.*, n. 215842; Cass., sez. un., sent. 21 giugno 2000 n. 16, Tammaro, in *CED Cass.*, n. 216249.

[13] D.lgs. 30 maggio 2008 n. 109, recante «Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE».

za risposta per settantadue mesi. È evidente che, di fatto, i *service providers* conserveranno i dati per settantadue mesi perché non possono sapere per quale tipo di reato si chiederà l'acquisizione[14]. Poi, a seconda del tipo di reato per cui si procede si potrà risalire nel tempo di settantadue mesi ovvero ventiquattro-dodici mesi o trenta giorni.

Per quanto riguarda, invece, la disciplina dell'acquisizione di tali dati, inizialmente l'art. 132, co. 2 codice *privacy* prevedeva che i tabulati venissero acquisiti con provvedimento del giudice su richiesta del pubblico ministero[15] mentre, per effetto della modifica introdotta con il d.l. 27 luglio 2005 n. 144, convertito con modificazioni nella legge 31 luglio 2005 n. 155, la potestà acquisitiva era tornata nelle mani del solo pubblico ministero.

Da ultimo, l'art. 132 codice *privacy*, nella parte relativa alle modalità di acquisizione dei dati, è stato novellato dal d.l. 30 settembre 2021 n. 132, convertito con modificazioni dalla l. 23 novembre 2021 n. 178, per adeguare il diritto interno ai principi espressi dalla Corte di giustizia nella sentenza *Prokuratuur* del 2 marzo 2021. In particolare, il novellato co. 3 prevede che i dati relativi al traffico telefonico e telematico possano essere acquisiti – previa autorizzazione rilasciata dal giudice su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa o delle altre parti private – se sussistono sufficienti indizi di reato, purché si tratti di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'art. 4 c.p.p., e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia o il disturbo sono gravi e i dati siano rilevanti per l'accertamento dei fatti.

Il co. 3-*bis* introduce, sulla falsa riga di quanto previsto in materia di intercettazioni, una disciplina specifica per il caso in cui emerga la necessità di acquisire i tabulati telefonici con urgenza e vi sia fondato motivo di ritenere che dal ritardo possa derivare un grave pregiudizio alle

[14] S. MARCOLINI, *La disciplina processuale italiana sul* data retention, in R. FLOR, S. MARCOLINI (a cura di), *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quali limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Torino, 2022, p. 47.

[15] Come previsto dall'art. 3 d.l. 24 dicembre 2003 n. 354.

indagini, consentendo in questo caso al pubblico ministero, sussistendo i presupposti di cui sopra, di acquisire i dati di traffico con decreto motivato che deve essere comunicato immediatamente, e comunque non oltre le quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria (il quale dovrà, entro le quarantotto ore successive, decidere sulla convalida con decreto motivato). La norma non lo dice, ma sembra potersi concludere, per analogia con quanto disposto dall'art. 266, co. 2 c.p.p. che, nel caso in cui il giudice non convalidi l'acquisizione urgente, i dati *medio tempore* acquisiti siano inutilizzabili. Infine, il co. 3-*quater* prevede espressamente la sanzione di inutilizzabilità per i tabulati acquisiti in violazione delle disposizioni dei co. 3 e 3-*bis*.

Quindi, sono inutilizzabili i tabulati acquisiti sia al di fuori dei presupposti, sia oltre i limiti massimi di conservazione.

In sede di conversione con l. 23 novembre 2021 n. 178 il legislatore ha introdotto, inoltre, una disciplina transitoria relativa al regime di utilizzabilità dei dati di traffico acquisiti nei procedimenti penali in data anteriore all'entrata in vigore della novella, ossia al 30 settembre 2021, stabilendo che gli stessi possano essere utilizzati a carico dell'imputato solo per l'accertamento dei reati che rientrano nel neo-introdotto catalogo e solo unitamente ad altri elementi di prova.

3. Compatibilità con la disciplina europea: il rinvio pregiudiziale del giudice per le indagini preliminari di Bolzano

Con l'ultimo intervento normativo il legislatore italiano si è adeguato ai principi espressi dalla Corte di giustizia, nella misura in cui ha limitato il novero dei reati per cui è possibile acquisire i tabulati e ha previsto che l'autorizzazione provenga dal g.i.p. su richiesta del pubblico ministero (caso più frequente) o del difensore della persona sottoposta alle indagini o della persona offesa.

A seguito della novella ci si è chiesti se il legislatore avesse dato piena e corretta attuazione alle indicazioni della Corte di Lussemburgo.

Oltre alle critiche espresse dalla dottrina[16], anche la giurisprudenza ha manifestato perplessità sulla compatibilità del nuovo assetto normativo con il diritto dell'Unione.

Infatti, il giudice per le indagini preliminari presso il Tribunale di Bolzano ha sollevato una questione pregiudiziale che ha poi portato alla sentenza della grande sezione della Corte di giustizia del 30 aprile 2024[17].

In particolare, nel rinvio pregiudiziale il g.i.p. di Bolzano dubitava della compatibilità del novellato art. 132 codice *privacy* con l'art. 15, § 1 della direttiva 2002/58/CE in quanto, nell'individuare il catalogo dei reati gravi facendo riferimento a quelli puniti con la pena della reclusione non inferiore nel massimo a tre anni, il legislatore non avrebbe rispettato il principio di proporzionalità sancito dall'art. 52 Carta dir. fond. UE. Inoltre, secondo il giudice rimettente, il legislatore italiano non avrebbe lasciato alcuna discrezionalità al giudice nel valutare se autorizzare l'acquisizione dei tabulati o meno, essendo l'autorizzazione obbligata al ricorrere dei presupposti previsti dalla legge, ossia la sussistenza di sufficienti indizi di reato e la rilevanza per l'accertamento dei fatti.

La Corte di giustizia, con la sentenza del 30 aprile 2024, conformemente alla sua tradizionale giurisprudenza, ha innanzitutto ribadito che, tenuto conto della ripartizione di competenze tra l'Unione e gli Stati contraenti ai sensi del Trattato funz. UE e delle notevoli differenze esistenti tra gli ordinamenti giuridici nazionali nella materia penale, spetta agli Stati membri definire i "reati gravi" ai fini dell'applicazione dell'art. 15 § 1 della direttiva 2002/58/CE.

---

[16] S. MARCOLINI, *La disciplina processuale italiana sul data retention*, cit., p. 62 secondo cui il rinvio a reati puniti con la pena della reclusione non inferiore nel massimo a tre anni costituisce un rinvio a una categoria troppo ampia di reati, essendo stato preferibile che il legislatore limitasse la possibilità di acquisire i tabulati ai soli reati previsti dall'art. 407, co. 2 lett. a) c.p.p.

[17] CGUE, grande sezione, sent. 30 aprile 2024, causa C-178/22, Ignoti con l'intervento di Procura della Repubblica presso il Tribunale di Bolzano. Si veda G. TODARO, *L'evoluzione delle fonti del diritto nella «società algoritimica»:* data retention *e diritti fondamentali della persona*, in *Cass. pen.*, 2024, p. 2035.

A tal fine, secondo la Corte di Lussemburgo, il criterio utilizzato dal legislatore italiano, ossia quello di definire i "reati gravi" facendo riferimento alla pena in astratto prevista per gli stessi, è da intendersi come un criterio oggettivo.

Tuttavia, si legge nella sentenza, poiché il legislatore italiano ha individuato i reati gravi facendo riferimento a un minimo di pena massima applicabile e non alla pena minima, potrebbe accadere che un accesso ai dati esterni di una comunicazione, che secondo la Corte di giustizia rappresenta una grave ingerenza nei diritti fondamentali, possa essere richiesto anche in relazione a reati che in realtà non rientrano tra le forme di criminalità grave. E quindi, poiché la definizione di "reati gravi" fornita dagli Stati Membri deve rispettare i dettami dell'art. 15, § 1 letto alla luce degli artt. 7, 8 e 11 nonché dell'art. 52, § 1 Carta dir. fond. UE e poiché, in particolare, l'art. 15, § 1 della direttiva individua tra i principi a cui la disciplina nazionale deve ispirarsi per essere conforme al diritto europeo, quello di proporzionalità, occorre che il giudice nazionale possa negare o limitare l'accesso ai tabulati qualora constati che l'ingerenza nei diritti fondamentali che un tale accesso costituirebbe è grave, anche se risulta evidente che il reato in questione non rientra effettivamente nella criminalità grave.

Secondo la Corte di giustizia il giudice deve quindi essere in grado di garantire un giusto equilibrio tra gli interessi legittimi connessi alle esigenze dell'indagine nell'ambito della lotta alla criminalità e i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali di coloro i cui dati sono interessati dall'accesso. In particolare, allorché si trova a esaminare la proporzionalità dell'ingerenza nei diritti fondamentali della persona interessata causata dalla richiesta di accesso ai tabulati, tale giudice deve essere in grado di escludere detto accesso qualora quest'ultimo sia richiesto nell'ambito di un'azione penale diretta a perseguire un reato manifestamente non grave.

Si tratta essenzialmente dell'applicazione del controllo di proporzionalità in concreto.

Il principio di proporzionalità, infatti, pervade di sé l'ordinamento processuale penale ed è applicabile ogni qualvolta un'attività di indagine incida su diritti fondamentali, come nel caso dell'acquisizione dei tabulati telefonici e telematici.

Secondo la dottrina[18], infatti, gli indici rivelatori della necessità di realizzare il controllo di proporzione sono i seguenti:

1. la messa a repentaglio di un diritto inviolabile;
2. una base probatoria (presupposto sostanziale);
3. un'esigenza processuale al cui servizio si pone la limitazione legale del diritto individuale (presupposto cautelare).

L'art. 132, co. 3 codice *privacy* nell'attuale formulazione, introdotta nel 2021, contiene tutti gli indici rivelatori della necessità di attuare il controllo di proporzione:

1. l'acquisizione dei dati di traffico telefonico e telematico incide su diritti fondamentali (il diritto al rispetto della vita privata);
2. proprio per questo motivo la norma richiede che per l'acquisizione dei tabulati, il giudice valuti in primo luogo la sussistenza di un fatto-reato, qualificandolo giuridicamente, del quale vi siano sufficienti indizi e che l'acquisizione sia rilevante per l'accertamento dei fatti (presupposto sostanziale). Si noti che il giudizio di "rilevanza" qui richiesto, oltre a essere ispirato al principio di proporzionalità, è anche più rigoroso di quello previsto dall'art. 190 c.p.p. quale criterio generale per l'ammissione della prova da parte del giudice: nel dibattimento, infatti, il giudice può escludere le prove richieste dalle parti solo se «manifestamente irrilevanti»;
3. infine, il giudice dovrà valutare quale sia l'esigenza processuale al cui servizio si pone la limitazione legale del diritto individuale (presupposto cautelare) e quindi stabilire se il sacrificio dei diritti fondamentali sia giustificato alla luce dell'obiettivo da perseguire, ovvero se lo stesso sia perseguibile con strumenti di indagine meno invasivi.

Il giudice dovrà quindi motivare nel suo provvedimento, alla luce di questi parametri, il motivo per cui ha ritenuto di autorizzare l'acquisizione di quei dati, applicando un controllo di proporzionalità in concreto, ossia valutando la necessità, idoneità e proporzionalità in senso stretto dell'acquisizione dei tabulati rispetto al fatto-reato per cui si sta procedendo.

[18] M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Diritto penale contemporaneo - Rivista trimestrale*, 2014, 3/4, p. 143.

Peraltro, la disciplina italiana dell'acquisizione dei tabulati telefonici e telematici segue lo stesso schema riproposto nelle norme relative alle intercettazioni, seppur con requisiti meno stringenti. Ciò in considerazione della valutazione, condivisa dalla giurisprudenza nazionale, della minor lesione del diritto al rispetto della vita privata determinata dall'acquisizione dei tabulati telefonici rispetto a quella che si determina per effetto delle intercettazioni.

Questa conclusione non è condivisa dalla dottrina, secondo cui, al contrario, l'acquisizione dei tabulati per un periodo di settantadue mesi, come è previsto per i reati di cui all'art. 51, co. 3-*quater* e 407, co. 2 lett. a) c.p.p., può rivelare molto di più della vita privata di una persona rispetto a un'intercettazione telefonica di pochi giorni; si è inoltre evidenziato come la categoria dei "reati gravi" individuata dal legislatore sia troppo ampia[19].

4. La questione (irrisolta) della conservazione dei dati di traffico telefonico e telematico

Il vero problema che si pone oggi in maniera urgente è quali siano gli effetti nell'ordinamento nazionale della sentenza della Corte di giustizia del 5 aprile 2022, nella parte in cui afferma che la conservazione generalizzata e indifferenziata dei dati di traffico telefonico, telematico e relativi alle chiamate senza risposte è incompatibile con l'art. 15 § 1 della direttiva 2002/58/CE, alla luce degli articoli 7, 8 e 11 e dell'art. 52, § 1 Carta dir. fond. UE.

Infatti, l'art. 132, co. 1 e 1-*bis* codice *privacy* prevede obblighi di conservazione generalizzata e indifferenziata di tali dati c.d. esterni di una comunicazione telefonica o telematica ed è pertanto incompatibile con il diritto dell'Unione.

Le conseguenze di tale incompatibilità sono quelle ricordate dalla Corte di giustizia al § 118 della sentenza in questione. Il principio della *primauté* del diritto dell'Unione impone a tutte le istituzioni degli Stati membri di dare piena efficacia alle varie disposizioni del diritto euro-

[19] S. MARCOLINI, *La disciplina processuale italiana sul data retention*, cit., p. 62.

peo e, quindi, ove non sia possibile procedere a un'interpretazione conforme del diritto nazionale, il giudice nazionale deve disapplicare la norma interna in contrasto con il diritto europeo, senza doverne chiedere o attendere la previa rimozione in via legislativa o mediante altro procedimento costituzionale. E l'effetto della disapplicazione, ricorda la Corte di Lussemburgo, non può che essere retroattivo, salva la possibilità, solo da parte sua e solo in via eccezionale, di prevedere nella sentenza una limitazione nel tempo degli effetti della pronuncia interpretativa; infatti,

> il primato e l'applicazione uniforme del diritto dell'Unione risulterebbero pregiudicati se i giudici nazionali avessero il potere di attribuire alle norme nazionali, anche solo provvisoriamente, il primato rispetto al diritto dell'Unione al quale esse contravvengono (§ 119).

L'art. 132, co. 1 e 1-*bis* codice *privacy* va pertanto disapplicato. Né si può salvare questa parte della disciplina nazionale alla luce delle modifiche normative introdotte sul piano dell'acquisizione dei dati di traffico. La Corte, infatti, sgombra il campo dall'idea che il recente adeguamento introdotto dal legislatore italiano in materia di acquisizione dei tabulati sia idoneo a limitare o a rimediare alla grave ingerenza nei diritti fondamentali alla vita privata e alla libertà di espressione che si verifica per effetto di una conservazione generalizzata e indifferenziata (§ 47).

Ma cosa significa nel caso concreto disapplicazione?

Analogamente ai problemi che si sono posti all'indomani della sentenza *Prokuratuur*, ci si deve interrogare sugli effetti di questa sentenza nell'ordinamento interno in relazione alle diverse fasi del procedimento penale, con una difficoltà aggiuntiva. Infatti, in questo caso non si tratta più soltanto di porsi nell'ottica del pubblico ministero che intenda acquisire i tabulati nella fase delle indagini (e del giudice per le indagini preliminari che deve autorizzare la relativa richiesta), domandandosi se sia ancora possibile acquisire i tabulati telefonici sulla base dell'art. 132 codice *privacy* pur sapendo che a monte non potevano essere conservati, o del giudice chiamato a decidere sull'utilizzabilità come prova ai fini del giudizio di colpevolezza dell'imputato di tabulati già acquisiti ma, prima ancora, del rapporto con i fornitori di servizi di comunica-

zione. Occorre quindi domandarsi se vi sia un onere per l'autorità giudiziaria di imporre a questi ultimi di non conservare indiscriminatamente i dati e di distruggere quelli conservati in epoca anteriore al 5 aprile 2022 e, in caso affermativo, sulla base di quale norma. Oppure se sia consentito ai singoli privati di chiedere, ai sensi dell'art. 7, co. 3 lett. b) codice *privacy*, la cancellazione dei dati che li riguardano e che risulterebbero, alla luce di quanto detto, illecitamente trattati.

Il tema risulta complesso e peculiare nel novero dei mezzi di ricerca della prova e delle sanzioni di inutilizzabilità proprio perché i dati non sono conservati su strumenti in uso alla procura della Repubblica, come nel caso delle intercettazioni, ma direttamente dai fornitori di servizi, con propri mezzi.

Risulta pertanto necessario un intervento del legislatore che adegui la disciplina italiana ai principi europei, tenendo conto delle indicazioni fornite dalla Corte di giustizia.

Occorrerà pensare a una normativa differenziata in base alla tipologia di dati da conservare; infatti, non è incompatibile con il diritto dell'Unione una disciplina che preveda la conservazione generica e indifferenziata degli indirizzi IP di una connessione e delle informazioni circa l'intestatario di un'utenza o di una connessione. Con riferimento ai dati di traffico e relativi all'ubicazione, secondo le indicazioni della Corte di giustizia, sarà necessario che la nuova disciplina legislativa circoscriva i dati da conservare in base a una particolare zona geografica o a una determinata cerchia di persone, introducendo criteri selettivi oggettivi e non discriminatori. Compito arduo, apparendo difficoltoso affermare, per esempio, che in una determinata zona d'Italia sia giustificata la conservazione dei dati di traffico e relativi all'ubicazione in quanto caratterizzata da un alto grado di criminalità grave, o che si possano conservare i tabulati di pregiudicati, senza incorrere in affermazioni discriminatorie.

Ma il problema non si riduce solo a questo. Occorrerà infatti stabilire come debbano fare, anche da un punto di vista tecnico, i *service providers* a conservare solo determinati dati e come veicolare loro l'informazione, per esempio, sui soggetti i cui dati possano essere conservati, senza informarli anche del motivo per cui sono stati selezionati. Non solo, ma bisognerà individuare dei meccanismi di aggiornamento pe-

riodico dei criteri selettivi. Più semplice probabilmente nell'ottica del legislatore utilizzare un criterio geografico, ma forse comunque tecnicamente difficile per i fornitori di servizi.

Infine, sempre seguendo le indicazioni della Corte di giustizia, appare opportuna l'introduzione positiva dell'ordine di congelamento, c.d. *quick freeze order* che permetterebbe, quanto meno dopo la notizia di reato di ordinare ai *service providers* di congelare i dati di traffico conservati per finalità di fatturazione in modo che siano utilizzabili per l'accertamento dei reati. Conservazione che, secondo quanto affermato dalla Corte di giustizia, potrebbe essere estesa a zone determinate quali i luoghi di commissione o preparazione del reato o a persone diverse da quelle sospettate di aver commesso un reato, ma che con queste abbiano avuto contatti in epoca antecedente alla commissione del reato. Il tutto ovviamente prevedendo la durata di tale conservazione rapida e le finalità per le quali può essere disposta.

Appare opportuno ricordare che l'art. 132, co. 4-*ter* codice *privacy* prevede già un ordine di congelamento, relativo ai soli dati di traffico telematico, nell'ambito delle investigazioni preventive. In particolare, consente al Ministro dell'Interno o, su sua delega, alle forze di polizia, di ordinare, anche su richiesta avanzata da un'autorità straniera, ai fornitori e agli operatori di servizi informatici e telematici la conservazione e protezione per un periodo non superiore a novanta giorni i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive ovvero per finalità di accertamento e repressione di specifici reati, prima dell'instaurazione di un procedimento penale.

È quindi necessario e urgente un intervento del legislatore che disciplini innanzitutto in modo specifico gli standard di sicurezza dei dati a cui devono assolvere i *service providers*. Sarebbe inoltre auspicabile la previsione di una disciplina transitoria, sulla falsa riga di quella introdotta in relazione ai tabulati acquisiti con solo provvedimento del pubblico ministero.

Medio tempore, bisognerebbe richiedere al giudice per le indagini preliminari l'emissione di un ordine di conservazione dei dati non appena si abbia notizia di un reato in relazione al quale si ritiene di avere necessità di acquisire i tabulati telefonici o telematici. Tale ordine, tut-

tavia, riguarderà i dati di traffico che si produrranno dall'ordine di congelamento in poi. Per quanto riguarda, invece, i tabulati antecedenti alla commissione del reato, si potrebbe pensare di estendere il *quick freeze order* ai dati di traffico conservati per finalità di fatturazione, in modo che siano utilizzabili per l'accertamento dei reati.

5. Riflessione: il ruolo del pubblico ministero alla luce del diritto europeo

La disciplina dell'acquisizione dei tabulati telefonici e telematici costituisce il banco di prova dei rapporti, *rectius*, delle tensioni tra diritto nazionale e diritto sovranazionale, nonché lo spunto per una riflessione su come il diritto europeo/sovranazionale, laddove si occupa del bilanciamento tra diritti fondamentali ed esigenze di accertamento e repressione dei reati, sia in grado di incidere anche su aspetti ordinamentali, quali quelli che attengono al ruolo del pubblico ministero.

Infatti, secondo la Corte di giustizia l'ingerenza che la conservazione e acquisizione dei tabulati telefonici e telematici determina nel diritto alla vita privata è grave e, pertanto, è necessario che sia autorizzata da un'autorità terza rispetto alle parti del processo penale.

Questo modo di ragionare non tiene tuttavia conto del fatto che, se è senz'altro vero che il pubblico ministero non è terzo, è altresì vero che nel nostro ordinamento il pubblico ministero è indipendente ed è tenuto a svolgere le indagini anche a favore della persona indagata. Questi principi giustificano i poteri di limitazione di diritti fondamentali, riconosciuti al pubblico ministero italiano quando si tratta di disporre una perquisizione o un sequestro.

Ed è per queste stesse ragioni che la giurisprudenza della Corte di Cassazione, ma anche della Corte costituzionale, nel distinguere tra diritto alla segretezza delle comunicazioni e diritto alla riservatezza, ha tradizionalmente considerato la limitazione della riservatezza meno grave di quella della segretezza, ritenendo nel secondo caso sufficiente quel "livello minimo di garanzie" costituito dal decreto motivato del pubblico ministero.

Questo ragionamento, però, non è più sostenibile alla luce dei principi di derivazione sovranazionale espressi nella giurisprudenza della Corte di giustizia che ha chiaramente affermato la necessità di tenere alto il livello di garanzie in tutti i casi di acquisizione di dati di traffico, impostazione questa che pare avere sposato anche il nostro legislatore nella stesura del disegno di legge avente ad oggetto la disciplina di perquisizioni e sequestri informatici, laddove ha previsto che l'acquisizione dei dati informatici avvenga mediante decreto di sequestro del giudice su richiesta del pubblico ministero[20].

[20] D.d.l. n. 806 del 19 luglio 2023, recante «Modifiche al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici, *smartphone* e memorie digitali», su cui si rinvia al contributo di E. LORENZETTO nel presente volume.

CIRCOLAZIONE PROBATORIA INTERNA E TRANSFRONTALIERA

NOTE INTRODUTTIVE

Giulio Illuminati

Stando ai dati riportati in un recente articolo di Filippo Spiezia, la prova digitale è rilevante in circa l'85% delle indagini penali, e nel 65% dei casi (vale a dire, il 55% del totale) per acquisirla occorre rivolgere una richiesta a un *service provider* basato all'estero. Questo conferma, se mai ce ne fosse bisogno, l'importanza dell'argomento di questa sessione, la circolazione della prova digitale.

Ora, a prescindere da una precisa definizione del concetto di prova digitale – che in realtà abbraccia una grande varietà di dati informatici o informatizzati, anche piuttosto distanti fra loro quanto a caratteristiche – appare evidente che bisogna prendere atto di una progressiva mutazione della originaria struttura della prova e del processo penale, a suo tempo focalizzato sui principi di oralità, immediatezza e contraddittorio. Infatti, la prova per eccellenza ormai non è più la testimonianza, come sanno gli operatori pratici, e di conseguenza le nostre usuali categorie rischiano di sbandare, poiché ci troviamo di fronte a una serie di elementi nuovi, particolarmente significativi, che sono anche difficili da inquadrare.

Per altro verso, la legge non riesce, come sempre accade, a tener dietro ai rapidi sviluppi della tecnologia: basti ricordare, nel nostro caso, che il codice è entrato in vigore in un'epoca in cui le intercettazioni si eseguivano mediante una derivazione fisica dalla centrale telefonica, si ascoltavano in tempo reale, e il contenuto delle comunicazioni intercettate veniva riversato su nastro magnetico (che ancora molto di recente, prima delle ultime riforme, era menzionato appunto come tale nel codice).

Anche il concetto stesso di comunicazione oggi non è chiarissimo, tanto che assistiamo spesso a disorientamenti della giurisprudenza. Ho ascoltato con grande interesse la relazione di Alberto Camon e gli esempi che ci ha portato: potrei farne di altri, ma comincio a domandarmi se non sia il caso di abbandonare l'idea di poter prendere in considerazione le sole comunicazioni in senso stretto.

È vero che l'art. 15 Cost. parla testualmente di libertà e segretezza delle comunicazioni, però oggi il concetto si deve necessariamente ampliare, perché comunicazione non è soltanto il contenuto di una conversazione intercettata, ma anche per esempio – è stato detto questa mattina – i metadati, attraverso i quali è possibile profilare un soggetto; mentre è irrilevante il fatto che si tratti di comunicazioni captate in tempo reale o dati immagazzinati in un qualsiasi dispositivo. È inutile, in altre parole, continuare a domandarsi se nel caso specifico si tratti di sequestro, perquisizione, o intercettazione, o addirittura di prova atipica – come spesso preferisce definirla la giurisprudenza – erroneamente considerata non soggetta a regole di ammissione. Lungi da me l'idea di formulare una definizione omnicomprensiva, ma forse si dovrebbe semplicemente cominciare a parlare, in termini generalissimi, di sorveglianza elettronica, in tutte le sue varie forme. Come accade, per esempio, in altri paesi: in Germania, lo sappiamo, il *Bundesverfassungsgericht* ha dedotto i limiti costituzionali alla possibilità di sorveglianza elettronica delle persone, assunta come categoria generale, dal principio della tutela della dignità umana e del libero sviluppo della personalità individuale. L'art. 8 Conv. eur. dir. uomo include nel più ampio diritto al rispetto della vita privata e familiare la tutela della corrispondenza; analogamente si comporta, con l'art. 7, la Carta dei diritti fondamentali dell'UE, che inoltre aggiunge, all'art. 8, la previsione specifica del diritto alla protezione dei dati personali.

Anche la Corte costituzionale italiana, a suo tempo, ha avuto modo di pronunciarsi, sia pure in un *obiter dictum* (sentenza n. 173 del 2009), sul diritto alla riservatezza, ritenuto un diritto fondamentale «riguardante la vita privata dei cittadini nei suoi molteplici aspetti», che si basa sugli artt. 2 e 15 Cost. Si parla spesso, oggi, di 'nuovi diritti', poiché secondo alcuni il testo della Costituzione non copre tutte le manifestazioni della personalità individuale; ma, come è stato evidenziato, quan-

do si parla di nuovi diritti in realtà si fa riferimento a nuove manifestazioni di un diritto già riconosciuto dalla Costituzione, ovvero a diritti che risultano dalla combinazione di altri principi costituzionali preesistenti.

A questo proposito, vorrei fare rinvio – dando per nota la giurisprudenza europea, di cui si è già parlato – alla motivazione di una ormai antica sentenza della Corte costituzionale in tema di intercettazioni telefoniche, la n. 34 del 1973, e mi fa piacere che questa mattina Gabriella Di Paolo l'abbia menzionata, perché è sempre stato uno dei miei punti di riferimento primari. Ho annotato una serie di principi enunciati da quella sentenza – che, rammento, è giusto di cinquanta anni fa – principi che sono ancora oggi validi, nonostante siano stati dettati nella vigenza del codice abrogato, e che vanno, secondo me, considerati applicabili a tutti i tipi di interferenza nella vita privata.

Anzitutto il bilanciamento tra diritto alla segretezza delle comunicazioni – ma possiamo a questo punto parlare anche di diritto alla riservatezza – e l'esigenza di prevenire e reprimere i reati, anch'essa oggetto, si afferma, di protezione costituzionale (si potrebbe magari discutere, ma qui è irrilevante, sui criteri di questo bilanciamento, che a mio modo di vedere non può mai essere paritario). Inoltre, la necessità di un'autorizzazione del giudice, con una motivazione che dia conto del bilanciamento effettuato; la previsione di limiti di durata dell'intercettazione. Soprattutto, poi, il principio di proporzionalità, oggi com'è noto diventato centrale: ne parliamo di solito come di un'acquisizione derivante dalla giurisprudenza europea, e in parte è così, ma va sottolineato che già a quel tempo la Corte costituzionale ne aveva riconosciuto il valore. Infine, la necessità di garanzie di ordine tecnico, particolarmente importanti perché è indispensabile assicurare l'autenticità dei dati e l'integrità nella loro conservazione.

C'è infatti da rimanere perplessi quando il legislatore promette per esempio di attribuire alla polizia giudiziaria il compito di tagliare le intercettazioni non rilevanti: chi decide la rilevanza, la polizia? E alla fine chi lo fa il processo, la polizia? Si afferma che escludere le intercettazioni irrilevanti serve a tutelare la riservatezza dei soggetti coinvolti, ma in questi termini il rimedio è quantomeno sproporzionato. In ogni caso poi, come ho avuto occasione di scrivere altrove, il risultato delle

intercettazioni non è altro che una prova indiziaria, che spesso può essere ambigua e persino fuorviante, che spesso non è nemmeno correttamente conservata, che spesso si basa su trascrizioni non fedeli e imprecise, su traduzioni e interpretazioni erronee o, appunto, pregiudicate dall'eventuale esclusione di brani di conversazione che potrebbero invece essere rilevanti.

Dunque, nella motivazione di quella storica sentenza viene detto già tutto: inclusa l'esigenza del controllo di rilevanza dei risultati; del controllo di legittimità dell'operazione; della tutela del segreto; e, in particolare, anche l'esigenza della tutela dei terzi. Va poi evidenziato, ma su questo non mi soffermo, che vi si parla per la prima volta di inutilizzabilità della prova illegittimamente acquisita – solo più tardi introdotta con la riforma del codice – con un passaggio celebre che vale comunque la pena citare, secondo cui dall'art. 15, co. 1 Cost. è possibile inferire

> il principio secondo il quale attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione e a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito.

La verità è che le intercettazioni, come pure tutte le forme di sorveglianza elettronica, si collocano in un crocevia di interessi in conflitto: da un lato l'esigenza di svolgere le indagini e del segreto investigativo (non entro qui nell'argomento, spesso agitato in maniera pretestuosa, del numero eccessivo di intercettazioni, oppure del requisito dei gravi indizi di colpevolezza o gravi indizi di reato); dall'altro la tutela della segretezza delle comunicazioni e della riservatezza personale; per altro verso, il diritto di cronaca, del quale ha avuto più di una volta occasione di occuparsi la Corte europea, secondo cui la riservatezza non può essere invocata a fronte dell'art. 10 Conv. eur. dir. uomo sulla libertà di espressione quando si tratta di un personaggio politico pubblico (il che fra l'altro fa giustizia di certe polemiche nostrane di questi giorni); infine, ma non per ultima, la tutela del diritto di difesa.

A questo punto appare chiaro che la garanzia costituzionale deve abbracciare tutte le possibili forme di interferenza nella vita privata: a partire dalle riprese visive, per le quali manca completamente un qua-

dro normativo, e che pertanto sono ai limiti della legalità, nonostante le acrobazie della giurisprudenza, ordinaria e anche costituzionale, per salvarle almeno in parte; e fino al captatore informatico, le cui potenzialità invasive sono enormi.

Al di là dell'intercettazione di comunicazioni in senso stretto, ho provato a fare un elenco delle possibili interferenze, probabilmente non esaustivo: l'intercettazione di flussi di dati; la conservazione dei dati esterni delle comunicazioni (*data retention*); la remotizzazione degli ascolti; l'instradamento delle comunicazioni internazionali; le ispezioni e perquisizioni informatiche; l'acquisizione della messaggistica istantanea, criptata o no; il sequestro della memoria del dispositivo; la geolocalizzazione; il *pen register*, che tiene traccia di tutte le chiamate in uscita; lo *stingray*, simulatore di telefono cellulare, sia attivo che passivo. E, come sappiamo, oggi il captatore informatico – che il nostro legislatore prevede (ingenuamente?) solo per l'intercettazione di comunicazioni tra presenti – ha la possibilità di prendere possesso del dispositivo con i privilegi di amministratore, con tutto ciò che ne consegue in termini di sorveglianza elettronica.

Per questo motivo non condivido quello che è diventato una sorta di luogo comune: si usa parlare di 'neutralità tecnica' delle norme di garanzia, sarebbe cioè indifferente lo strumento che viene usato, purché sia tutelato il nucleo essenziale del diritto che deve essere riconosciuto. Ma in realtà c'è una enorme differenza, per esempio, fra l'intercettazione di una comunicazione, la ripresa visiva, il virus informatico inserito nel cellulare, e così via. Il tipo di strumento condiziona gli effetti e i risultati, e le garanzie debbono essere tarate sulle modalità e sull'obiettivo. Al riguardo, ancora dalla Corte costituzionale tedesca, è stato affermato il cosiddetto *purpose limitation principle*, vale a dire il principio secondo cui l'intervento deve essere limitato in funzione del legittimo scopo che viene perseguito.

A questo punto è facile il collegamento con l'argomento di questa sessione. Anche sulla circolazione dei dati da un procedimento all'altro occorre, secondo me, tener presente che ogni volta che si utilizza un dato di questo genere si realizza una nuova violazione della segretezza, che deve trovare giustificazione. Non basta l'esistenza di un'autorizzazione a monte per concludere che il diritto è sufficientemente tutelato.

L'utilizzazione in altra sede deve sempre restare un'eventualità eccezionale, perché l'autorizzazione originaria, emessa in un contesto differente, non può rappresentare un *passepartout* mediante il quale la prova risulta una volta per tutte legittimata ed è possibile usarla dovunque e a qualunque fine. E l'osservazione diventa di particolare attualità se si pensa alla ben nota vicenda dei criptofonini e alla trasmissione, richiesta con ordine europeo di indagine, del contenuto di comunicazioni già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti a essa.

Il legislatore, con le modifiche all'art. 270 c.p.p., aveva fatto un gran pasticcio, perché il testo originario prevedeva che l'utilizzazione in procedimenti diversi fosse consentita solo per i reati suscettibili di arresto obbligatorio in flagranza, ma poi era stato aggiunto quel riferimento posticcio ai reati previsti dall'art. 266 c.p.p., che qualcuno con grande buona volontà ha provato a interpretare come limite inteso a escludere quei reati ad arresto obbligatorio che non fossero previsti nell'elenco dell'art. 266, nonostante il tenore letterale facesse pensare piuttosto a un allargamento praticamente a tutti i reati per i quali l'intercettazione risulterebbe consentita. La modifica è infine giustamente caduta in sede di conversione del decreto-legge (lasciando peraltro strascichi di diritto transitorio), ma dà un'idea dell'approssimazione con cui lavorano il governo e le maggioranze parlamentari.

Quanto detto in precedenza vale anche, per esempio, per la disciplina, completamente nuova, del captatore informatico. Ci si può domandare come sia possibile che nessuno abbia pensato di regolamentarne separatamente le molteplici possibili finalità, limitandosi invece, come ho già accennato, a contemplare la sola funzione di intercettazione delle comunicazioni tra presenti. O meglio, qualcuno ci aveva pensato, e mi riferisco al progetto di legge Quintarelli, che molti dei presenti conosceranno, ma che è stato immediatamente messo da parte.

E concludo ricordando che dobbiamo anche evitare di cadere in quello che qualcuno ha acutamente definito 'pregiudizio tecnologico', a causa del quale si tende a considerare i dati acquisiti con questo tipo di strumenti come dati oggettivi e inconfutabili, validi ovunque. Non è così, lo dicevo prima: si tratta soltanto di indizi, e a volte nemmeno indizi, ma semplici notizie di reato.

In ogni caso le prove vanno cercate senza commisurarle all'obiettivo di prendere di mira una qualsiasi persona. Già negli anni Sessanta del secolo scorso, erano espressamente vietate, negli Stati Uniti, quelle che venivano chiamate intercettazioni generali, dirette cioè a mettere sotto sorveglianza un sospettato in attesa di scoprire qualche elemento a suo carico: dal momento che è sempre necessario che esistano specifici motivi che giustifichino la restrizione del diritto fondamentale. In linea di principio, dunque, deve escludersi che le intercettazioni possano essere impiegate per andare alla ricerca di possibili reati. E la medesima logica va applicata anche, *mutatis mutandis*, all'utilizzazione delle intercettazioni al di fuori del procedimento in cui sono state autorizzate. Altrimenti, come ha di recente riconosciuto anche la Corte costituzionale, si tratterebbe di un'autorizzazione in bianco, priva cioè del suo requisito essenziale, una motivazione pertinente e specifica.

LA CIRCOLAZIONE DEGLI ESITI DELLE INTERCETTAZIONI IN ALTRI PROCEDIMENTI INTERNI

I RIFLESSI DELLA SENTENZA DELLE SEZIONI UNITE "CAVALLO" SULLA GIURISPRUDENZA SUCCESSIVA

Luigi Giordano

SOMMARIO: *1. Il "recupero" del divieto di utilizzazione dei risultati delle intercettazioni in procedimenti diversi da quelli nei quali sono stati disposti. 2. Il divieto di utilizzo degli esiti delle intercettazioni per la prova dei reati "sotto soglia" emersi nello stesso procedimento. 3. Le successive "puntualizzazioni" della giurisprudenza di legittimità. 4. La determinazione del "perimetro" dell'autorizzazione del giudice. 5. Segue: la motivazione* per relationem *del provvedimento autorizzativo. 6. La modifica all'art. 270 c.p.p. ad opera della l. 28 febbraio 2020 n. 7 di conversione del d.l. 30 dicembre 2019 n. 161. 7. La determinazione dell'area operativa della nuova disposizione. 8. Segue: la sentenza Sezioni unite del 29 aprile 2024, Pisaniello e altri. 9. La nuova riforma dell'art. 270 c.p.p. intervenuta nel 2023. 10. Il deposito di verbali e registrazioni nel procedimento diverso. 11. Il particolare regime della circolazione dei risultati delle intercettazioni realizzate tramite* trojan*. 12. Segue: una diversa interpretazione dell'art. 270, co. 1-*bis *c.p.p.*

1. Il "recupero" del divieto di utilizzazione dei risultati delle intercettazioni in procedimenti diversi da quelli nei quali sono stati disposti

A distanza di qualche anno dal deposito della sentenza delle Sezioni unite "Cavallo" sull'interpretazione dell'art. 270 c.p.p.[1], è utile proce-

[1] Cass., sez. un., sent. 28 novembre 2019 n. 51/2020, Cavallo, in *Dir. pen. proc.*, 2020, 3, p. 357, con nota di G. PECCHIOLI, *Circolazione probatoria e intercettazioni: Le sezioni unite sull'annoso nodo gordiano*. Tra i tanti contributi sulla sentenza si vedano anche F. ALVINO, *La circolazione delle intercettazioni e la riformulazione dell'art. 270 c.p.p.: l'incerto pendolarismo tra regola ed eccezione*, in *Sistema penale*, 2020, 5, p. 233; G. DE AMICIS, *Il regime della "circolazione" delle intercettazioni dopo la ri-*

dere a una riflessione sulla sua portata e sulla sua influenza sulla giurisprudenza successiva.

Questa decisione ha recuperato uno spazio operativo al divieto di utilizzazione degli esiti delle intercettazioni in procedimenti diversi previsto dalla norma indicata. Tale divieto era stato sostanzialmente "sterilizzato" dalla giurisprudenza di legittimità prevalente.

La Corte di Cassazione, in particolare, ha precisato che il "legame sostanziale" tra il fatto-reato oggetto del decreto autorizzativo delle intercettazioni e quello emerso dagli ascolti, che permette di concludere che si tratti di reati relativi ad uno stesso procedimento, è ravvisabile solo nel caso in cui sussista una connessione tra gli stessi *ex* art. 12 c.p.p. La connessione, infatti, costituisce un legame che presenta carattere "sostanziale", ossia ha ad oggetto i fatti-reato indipendentemente dalle vicende procedimentali che possono riguardarli, e che è "originario", perché prende in considerazione rapporti tra reati sussistenti *ab origine*, cioè fin dalla loro commissione. Nel caso di imputazioni connesse, pertanto, il procedimento relativo al reato per il quale l'autorizzazione è stata espressamente concessa non può considerarsi "diverso" rispetto a quello relativo al reato accertato in forza dei risultati dell'intercettazione. Solo in questo caso non opera il divieto di cui all'art. 270 c.p.p.

A diverse conclusioni, e quindi all'applicazione del divieto, deve giungersi con riferimento alle ipotesi in cui sussiste solo un mero collegamento investigativo o probatorio tra i reati rilevante ai fini previsti dall'art. 371 c.p.p. Le figure di collegamento delineate da tale norma, difatti, riflettono la sola prospettiva dell'efficace conduzione delle indagini, non essendo espressione di un legame sostanziale tra i reati. La sola condizione che la prova di più reati derivi, anche solo in parte, dalla

forma, in *Cass. pen.*, 2020, p. 3526; G. ILLUMINATI, *Utilizzazione delle intercettazioni in procedimenti diversi: le Sezioni unite ristabiliscono la legalità costituzionale*, in *Sistema penale* (rivista web), 30 gennaio 2020 (ultimo accesso il 28 febbraio 2025); F. VANORIO, *Il permanente problema dell'utilizzo delle intercettazioni per reati diversi tra l'intervento delle sezioni unite e la riforma del 2020*, in *Sistema penale*, 2020, 6, p. 177 ss.; A. INNOCENTI, *Le Sezioni Unite limitano l'utilizzabilità dei risultati delle intercettazioni per la prova di reati diversi da quelli per cui sono state ab origine disposte*, in *Dir. pen. proc.*, 2020, 7, p. 993 ss.

stessa fonte, nella specie dalle stesse intercettazioni, pertanto, non rende utilizzabili gli esiti di intercettazioni disposte in altri procedimenti.

Con riferimento a quest'ultimo aspetto, l'interpretazione accolta dalle Sezioni unite si è distaccata dall'orientamento consolidato[2], incidendo in modo notevole sui procedimenti penali in corso così da provocare comprensibili valutazioni critiche della giurisprudenza di merito[3].

Tale cambiamento, tuttavia, affonda le sue radici nella inviolabilità delle comunicazioni, che può essere limitata solo per atto motivato dell'autorità giudiziaria[4]. Il margine di azione del divieto, in altri termini, è stato delineato facendo leva sull'elaborazione della Corte costituzionale sull'art. 15 Cost., tanto che è stato subito osservato che «le Sezioni unite hanno ristabilito la legalità costituzionale»[5].

L'art. 270, co. 1 c.p.p., che permette la circolazione dei risultati delle captazioni a iniziativa del pubblico ministero, pertanto, grazie alla

---

[2] Per l'affermazione secondo cui lo stesso procedimento che esclude l'applicazione del divieto di cui all'art. 270 c.p.p. presuppone che tra i fatti-reato, nonostante la differenza storica, sussista una connessione ex art. 12 c.p.p. o, comunque, un collegamento ex art. 371, co. 2, lett. b) e c), c.p.p., sotto il profilo oggettivo, probatorio e finalistico, che basta per ricondurre a unitarietà i procedimenti, cfr. tra le altre Cass., sez. III, sent. 24 aprile 2018 n. 29856, in *CED Cass.*, n. 275389 – 01; Cass., sez. III, sent. 28 marzo 2018 n. 46085, in *CED Cass.*, n. 275351 – 01; Cass., sez. III, sent. 5 novembre 2015 n. 2608, in *CED Cass.*, n. 266423 – 01.

[3] Cfr. Trib. Milano, sez. riesame, ord. 2 novembre 2020, in *Sistema penale* (rivista web), 1º dicembre 2020 (ultimo accesso il 28 febbraio 2025) con nota di D. ALBANESE, *Sull'utilizzabilità dei risultati delle intercettazioni nell'ambito del "medesimo procedimento": il Tribunale di Milano prende le distanze dalle Sezioni unite "Cavallo"*. In buona sostanza, è stato come se la Corte di legittimità avesse cambiato le regole del gioco durante la partita.

[4] Secondo le sezioni unite, la parziale coincidenza della re-giudicanda oggetto dei procedimenti connessi e, dunque, il legame sostanziale tra i diversi fatti-reato consente di ricondurre ai «fatti costituenti reato per i quali in concreto si procede» (così C. cost., sent. 11 luglio 1991 n. 366) valutati nel provvedimento autorizzatorio dell'intercettazione anche quelli oggetto delle imputazioni connesse che fossero stati accertati in forza dei risultati dello stesso mezzo di ricerca della prova, infatti, evita che il provvedimento del giudice si risolva in una sorta di "autorizzazione in bianco" al compimento di intercettazioni con conseguente lesione della "sfera privata" della libertà di comunicazione e del diritto di comunicare in modo riservato.

[5] G. ILLUMINATI, *Utilizzazione delle intercettazioni in procedimento diversi: Le Sezioni unite ristabiliscono la legalità costituzionale*, cit.

sentenza indicata è tornata a essere «una norma del tutto eccezionale»[6]: Solo reati particolarmente gravi giustificano l'uso di esiti intercettazioni svolte in un diverso procedimento nel quale non vi è stato un provvedimento motivato dell'autorità giudiziaria, in quanto

> la possibilità di utilizzare i risultati delle intercettazioni disposte nell'ambito di un determinato processo limitatamente ai procedimenti diversi, relativi all'accertamento di reati per i quali è obbligatorio l'arresto in flagranza, risponde all'esigenza di ammettere una deroga alla regola generale del divieto di utilizzazione delle intercettazioni in altri procedimenti, giustificata dall'interesse dell'accertamento dei reati di maggiore gravità[7].

2. Il divieto di utilizzo degli esiti delle intercettazioni per la prova dei reati "sotto soglia" emersi nello stesso procedimento

Le Sezioni unite, tuttavia, non fermandosi all'affermazione del principio illustrato, hanno affrontato anche una questione distinta, ma collegata a quella regolata dall'art. 270 c.p.p., concernente i limiti dell'impiego probatorio dei risultati delle intercettazioni per la prova di reati emersi nello stesso procedimento. A tal riguardo, la Corte ha concluso che queste comunicazioni o conversazioni sono utilizzabili come prova anche degli ulteriori fatti-reato emersi nello stesso procedimento[8] solo a condizione che tali delitti, a loro volta, rientrino nel catalogo previsto dall'art. 266 c.p.p.[9].

---

[6] Così C. cost., sent. 12 febbraio 1994 n. 63.

[7] Così C. cost., sent. 24 febbraio 1994 n. 63, richiamata da Cass., Sez. un., sent. 28 novembre 2019 n. 51, in *CED Cass.*, n. 277395 – 01.

[8] Secondo le Sezioni unite, dunque, indipendentemente dal numero di notizia di reato, lo stesso procedimento ricorrere quando il fatto-reato oggetto del provvedimento autorizzativo risulta legato a quello emerso dalle captazioni da una connessione sostanziale, rilevante ai sensi dell'art. 12 c.p.p.

[9] I risultati delle intercettazioni che esulassero dai limiti di ammissibilità sono comunque utilizzabili come *notitia criminis* (Cass., sez. II, sent. 13 dicembre 2016 n. 17759, in *CED Cass.*, n. 270219; Cass., sez. II, sent. 23 aprile 2010 n. 19699, in *CED Cass.*, n. 247104; Cass., sez. IV, sent. 3 ottobre 2006 n. 2596, in *CED Cass.*, n. 236115;

Questo secondo principio si è rivelato il profilo più criticato della decisione.

È stato sostenuto che le Sezioni unite avrebbero apposto, per via giurisprudenziale, un ulteriore limite all'utilizzabilità delle intercettazioni, non legislativamente previsto, né costituzionalmente imposto, per giunta in contrasto con altri principi costituzionali, rappresentati dal "principio di non dispersione degli elementi di prova" e dal "principio di uguaglianza". Una lettura costituzionalmente orientata all'art. 3 Cost. avrebbe dovuto portare verso una soluzione opposta a quella adottata dalle Sezioni unite: la sussistenza dei presupposti di cui all'art. 266 c.p.p. non dovrebbe essere ritenuta necessaria quando si procede per reati emersi dalle captazioni nel medesimo procedimento, purché le intercettazioni siano state *ab origine* legittimamente autorizzate[10].

La riserva di legge e di giurisdizione, inoltre, sarebbe stata assolta, anche per i reati non riconducibili all'art. 266 c.p.p. emersi "a valle" dell'attività captativa, dal controllo svolto dal giudice con riferimento al reato più grave (rientrante necessariamente nel catalogo *ex* art. 266 c.p.p.) in quanto a esso strettamente connessi *ex* art. 12 c.p.p.[11].

Cass., sez. V, del 2 maggio 2003 n. 23894, in *CED Cass.*, n. 225946; Cass., sez. VI, sent. 26 novembre 2002 n. 31, in *CED Cass.*, n. 225709).

[10] Le obiezioni di natura costituzionale poste alla soluzione accolta dalla sentenza delle Sezioni unite sono state riassunte in L. GIORDANO, *Inutilizzabilità dei risultati delle intercettazioni: diritti difensivi e prassi giurisprudenziali*, in P. MAGGIO (a cura di), *La nuova disciplina delle intercettazioni*, Torino, 2023, 368, dove si dà atto di una requisitoria della Procura generale della Corte di Cassazione, reperibile nel sito internet istituzionale, depositata nel procedimento definito con la sentenza Cass. sez. V, sent. 17 dicembre 2020 n. 1757, in *CED Cass.*, n. 280326.

[11] Cfr. A. INNOCENTI, *La Cassazione ribadisce l'applicabilità dei limiti generali di ammissibilità delle intercettazioni anche agli ulteriori reati emersi nello "stesso procedimento"*, in *Dir. pen. proc.*, 2021, 5, p. 630, il quale ritiene che «la tesi dell'inutilizzabilità dei risultati delle captazioni per la prova di quei reati che, seppur emersi nello "stesso procedimento", non soddisfano i limiti generali di ammissibilità di cui all'art. 266 c.p.p., non convince, in quanto si fonda su una lettura non condivisibile delle disposizioni costituzionali e delle sentenze della Consulta che a ben vedere tendono a evitare un "uso indiscriminato" delle risultanze delle intercettazioni ma non impongono una disciplina limitativa dell'utilizzabilità delle risultanze stesse nell'ambito dello "stesso procedimento", se legittimamente autorizzate ed eseguite».

Le successive pronunce della Corte di Cassazione, tuttavia, non si sono discostate dall'insegnamento delle Sezioni unite neppure su questo profilo[12]. Anzi, è stato affermato che l'esclusione dall'ambito di utilizzabilità degli esiti intercettativi i reati rientranti nel concetto di "stesso procedimento", ma non ricompresi nei limiti di ammissibilità di cui all'art. 266 c.p.p., costituisce una "piana applicazione" dell'art. 271 c.p.p. secondo cui i risultati delle intercettazioni sono inutilizzabili ove sia il prodotto di attività captative eseguite «fuori dai casi consentiti dalla legge», mentre la soluzione alternativa si tradurrebbe in un surrettizio aggiramento dei limiti normativi, con grave pregiudizio per gli interessi sostanziali tutelati dall'art. 266 c.p.p.[13].

Secondo la giurisprudenza di legittimità, in altri termini, l'autorizzazione del giudice a eseguire le intercettazioni per determinati reati non può essere usata come "un grimaldello" per travalicare il limite inderogabile stabilito dall'ordinamento[14].

Il criterio del "bilanciamento" tra valori costituzionali contrastanti, che ha ispirato la decisione delle Sezioni unite dapprima citata, impedisce che il principio di "non dispersione della prova" possa consentire di travalicare le garanzie offerte al diritto fondamentale della segretezza delle comunicazioni dalla "riserva" di legge di cui all'art. 15 Cost.

---

[12] Sul valore vincolante del precedente a Sezioni unite, si veda R. APRATI, *Cultura del dialogo e precedenti delle sezioni unite*, in *Cass. pen.*, 2021, p. 1241; cfr. anche la Relazione della Corte di Cassazione, Ufficio del massimario, n. 12 del 2021, *La vincolatività del precedente delle Sezioni Unite*, reperibile nel sito istituzionale nella quale è stato affermato che il vincolo *ex* art. 618 c.p.p. riguarda non solo il principio di diritto espresso in risposta al quesito oggetto dell'ordinanza di rimessione, ma anche quelle affermazioni – pregiudiziali o conseguenziali – che siano strettamente connesse a tale principio.

[13] Cass., sez. V, sent. 17 dicembre 2020 n. 1757, in *Dir. pen. proc.*, 2021, 5, p. 624, con nota di A. INNOCENTI, *La Cassazione ribadisce l'applicabilità dei limiti generali di ammissibilità delle intercettazioni anche agli ulteriori reati emersi nello "stesso procedimento"*, cit. e in *Sistema penale* (rivista web), 27 gennaio 2021, con nota di D. ALBANESE, *La Cassazione ritorna sui limiti all'utilizzabilità degli esiti delle intercettazioni nell'ambito del "medesimo procedimento": una parola definitiva, ma non per il futuro* (ultimo accesso il 28 febbraio 2025); di recente il principio è stato espresso da Cass., sez. V, sent. 13 giugno 2024 n. 40338, in *CED Cass.*, n. 287240; Cass., sez. V, sent. 28 maggio 2024 n. 34238, in *CED Cass.*, n. 286939.

[14] Cfr. Cass., sez. V, sent. 17 dicembre 2020 n. 1757, cit.

Non è stata ritenuta configurabile neppure la paventata compromissione dell'art. 112 Cost., perché la previsione di una regola processuale presidiata dalla sanzione di inutilizzabilità di cui all'art. 271 c.p.p. non incide sull'obbligo del pubblico ministero di esercitare l'azione penale, ma fissa i limiti di utilizzo di un mezzo di ricerca della prova particolarmente invasivo, con finalità di salvaguardia di un valore di rango costituzionale[15].

L'applicazione del principio espresso dalle Sezioni unite, peraltro, lascia una aporia: in taluni casi, nello stesso procedimento, una medesima base probatoria, al contempo, risulta utilizzabile per dimostrare la sussistenza di un reato e inutilizzabile per l'accertamento di altri reati[16]. È il caso, per esempio, degli esiti delle intercettazioni che potrebbero essere utilizzabili per dimostrare la sussistenza di una associazione per delinquere e non sarebbero impiegabili per la prova dei delitti scopo del sodalizio, che non rientrassero nei limiti di ammissibilità previsti dall'art. 266 c.p.p.[17].

Questa difficoltà manifesta il limite di fondo della soluzione accolta dalle Sezioni unite, che consiste nell'aver attribuito all'art. 266 c.p.p. una funzione che non gli è propria, quella di selezionare "a valle" in senso limitativo il materiale probatorio utilizzabile, ottenuto da un mezzo di

[15] Cfr. Cass., sez. V, sent, 17 dicembre 2020 n. 1757, cit.

[16] Cfr. F. VANORIO, *Il permanente problema dell'utilizzo delle intercettazioni per reati diversi tra l'intervento delle sezioni unite e la riforma del 2020*, cit., p. 184.

[17] Il reato di associazione per delinquere, ai sensi dell'art. 416, co. 1 c.p., permette l'impiego delle intercettazioni, le quali, pertanto, possono offrire elementi di prova su una serie potenzialmente indeterminata di delitti, anche non rientranti nell'elenco dei reati contemplati dall'art. 266 c.p.p., come le truffe semplici, i falsi non aggravati o diverse fattispecie di delitti tributari. Secondo l'indirizzo giurisprudenziale consolidato, è configurabile la continuazione, e, dunque, la connessione *ex* art. 12 c.p.p. che permette di ravvisare l'unicità del procedimento, tra il reato di partecipazione ad associazione criminale e i reati-fine nel caso in cui questi ultimi siano stati programmati al momento in cui il partecipe si è determinato a fare ingresso nel sodalizio, non essendo necessario che tale programmazione sia avvenuta al momento della costituzione dello stesso (cfr., tra le altre, Cass., sez. I, sent. 28 aprile 2023 n. 39858, in *CED Cass.*, n. 285369 – 01, in tema di partecipazione ad associazione mafiosa).

ricerca della prova legittimamente autorizzato, mentre la norma stabilisce una condizione di ammissibilità del mezzo di ricerca della prova[18].

3. Le successive "puntualizzazioni" della giurisprudenza di legittimità

I principi espressi dalle Sezioni unite sul tema della circolazione degli esiti delle captazioni sono stati successivamente sviluppati dalla giurisprudenza di legittimità.

La Corte di Cassazione, in particolare, ha specificato che i risultati delle intercettazioni autorizzate per la ricerca della prova di un determinato fatto-reato sono utilizzabili anche per dimostrare gli ulteriori fatti-reato legati al primo dal vincolo della continuazione *ex* art. 12, lett. b), c.p.p. senza che sia necessario che il disegno criminoso sia comune a tutti i correi[19]. La connessione derivante da unicità del disegno criminoso, che consente di escludere l'applicazione del divieto di cui all'art. 270 c.p.p., riconducendo a unitarietà il procedimento, deve sussistere tra i reati e non presuppone l'unicità dell'elemento volitivo di tutti gli agenti dei reati coinvolti[20].

---

[18] Cfr. A. INNOCENTI, *La Cassazione ribadisce l'applicabilità dei limiti generali di ammissibilità delle intercettazioni anche agli ulteriori reati emersi nello "stesso procedimento"*, cit., p. 633.

[19] Cass., sez. V, sent. 29 settembre 2021 n. 37697, in *CED Cass.*, n. 282027 – 01; Cass., sez. V, sent. 23 novembre 2021 n. 10671, in *CED Cass.*, n. 282862; Cass., sez. II, sent. 25 marzo 2022 n. 18248, inedita; Cass., sez. IV, sent. 13 aprile 2022 n. 28276, in *CED Cass.*, n. 283422; Cass., sez. IV, sent. 13 aprile 2022 n. 29924, inedita; Cass., sez. V, sent. 13 giugno 2022 n. 37459, inedita; Cass., sez. V, sent. 20 luglio 2022 n. 37922, inedita; Cass., sez. VI, sent. 18 ottobre 2022 n. 45879, inedita; Cass., sez. V, sent. 03 maggio 2023 n. 21902, inedita; Cass., sez. I, sent. 9 novembre 2023 n. 8909, inedita.

[20] Anche i risultati delle intercettazioni disposte per agevolare le ricerche di latitanti possono essere utilizzati a fini probatori con i limiti derivanti dal divieto di utilizzazione in procedimenti diversi di cui all'art. 270 c.p.p., il quale non opera, oltre che nei casi in cui l'attività captativa sia indispensabile per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza, nei procedimenti per reati connessi *ex* art. 12 c.p.p. a quelli in relazione ai quali tale attività era stata *ab origine* autorizzata, sempre che rientrino nei limiti di ammissibilità previsti dall'art. 266 c.p.p. (Cass., sez. II, sent. 17 set-

È stato poi aggiunto che la connessione *ex* art. 12, co. 1 lett. c), c.p.p., cioè l'ipotesi in cui il reato per cui si procede è stato commesso per eseguire od occultare gli altri, può sussistere anche se non fosse contestata l'aggravante di cui all'art. 61, co. 1 n. 2) c.p. Per esempio, sono utilizzabili nel procedimento relativo al delitto di favoreggiamento di un partecipe a un'associazione di tipo mafioso i risultati delle captazioni eseguite nel diverso procedimento relativo al delitto associativo concernente la medesima organizzazione, posto che tra i procedimenti sussiste il nesso di connessione teleologica *ex* art. 12, co. 1 lett. c), c.p.p., che rileva a prescindere dalla contestazione dell'aggravante di cui all'art. 61, co. 1 n. 2), c.p.[21].

Il divieto di cui all'art. 270, co. 1 c.p.p., peraltro, non opera quando la conversazione costituisce corpo del reato[22]. È corpo del reato, in quanto tale utilizzabile nel processo penale, solo allorché essa stessa integri ed esaurisca la condotta criminosa, nei casi in cui questa possa perfezionarsi anche con la sola interlocuzione oggetto di registrazione, mentre deve escludersi la natura di corpo del reato del dialogo intercettato che costituisca mera documentazione sonora della commissione del fatto[23].

I risultati della captazione correttamente autorizzata, inoltre, restano immuni rispetto al successivo sviluppo fisiologico del procedimento, atteso che in tal caso non rileva la sopravvenuta mancanza del presupposto legittimante per effetto della riqualificazione del fatto autorizza-

---

tembre 2021 n. 38831, in *CED Cass.*, n. 282199; Cass., sez. VI, sent. 18 settembre 2020 n. 26739, in *CED Cass.*, n. 279661).

[21] Cass., sez. I, sent. 4 luglio 2023 n. 48560, in *CED Cass.*, n. 285461 – 03.

[22] Cass., Sez. un., sent. 26 giugno 2014 n. 32697, in *Dir. pen. proc.*, 2014, p. 148, con nota di A. INNOCENTI, *Le Sezioni Unite aprono all'utilizzabilità dei risultati di intercettazioni disposte in "diverso procedimento"*.

[23] Cass., sez. VI, sent. 20 maggio 2021 n. 26307, in *CED Cass.*, n. 281536; Cass., sez. III, sent. 13 giugno 2024 n. 28723, in *CED Cass.*, n. 286730 – 01, in una fattispecie in cui la Corte ha ritenuto che costituissero corpo del reato di cui all'art. 615-*bis*, c.p., utilizzabili, come tali, nel processo penale i file captati in modalità attiva sul telefono cellulare dell'indagato contenenti immagini e video afferenti alla vita privata delle persone offese.

to[24]. Sono utilizzabili i risultati delle operazioni disposte in riferimento a un titolo di reato per il quale le stesse sono consentite, anche quando vi sia stata una successiva diversa qualificazione giuridica del fatto[25].

L'inutilizzabilità delle intercettazioni acquisite in violazione del divieto sancito dall'art. 270 c.p.p. ha natura "patologica" e, quindi, può essere rilevata anche nell'ambito del giudizio abbreviato[26]. Detto vizio, però, in difetto della previsione normativa della c.d. inutilizzabilità derivata, non inficia le deposizioni rese dagli interlocutori, cui sia stata data lettura delle conversazioni intercettate in ausilio alla memoria, in quanto essi, nel riferire quanto personalmente detto o ascoltato, diventano fonte di sommarie informazioni testimoniali[27].

---

[24] Cass., sez. VI, sent. 20 gennaio 2021 n. 23244, in *Giur. it.*, 2021, p. 2469, con nota di A. INNOCENTI, *Sono utilizzabili le intercettazioni in caso di ''fisiologica'' riqualificazione del reato*. La legittimità di una intercettazione deve essere verificata al momento in cui la captazione è richiesta e autorizzata, non potendosi procedere al controllo della sua ritualità sulla base delle risultanze derivanti dal prosieguo delle captazioni e dalle altre acquisizioni (Cass., sez. VI, sent. 30 marzo 2023 n. 22390, inedita; Cass., sez. VI, sent. 1º marzo 2016 n. 21740, in *CED Cass.*, n. 266922). Il mutamento dell'addebito, anche per effetto della esclusione di una circostanza aggravante, che intervenga nel corso del fisiologico sviluppo del procedimento, non determina la inutilizzabilità dei risultati dell'attività tecnica, la quale consegue solo se i presupposti per disporre le captazioni mancassero al momento di autorizzazione delle stesse (Cass., sez. VI, sent. 12 aprile 2022 n. 48320, in *CED Cass.*, n. 284074 – 01). L'utilizzabilità degli esiti delle intercettazioni, tuttavia, è condizionata alla sussistenza, al momento dell'emissione del decreto autorizzativo, dei presupposti per l'autorizzazione del mezzo di ricerca della prova (cfr. Cass., sez. VI, 20 gennaio 2021 n. 23148, Bozzini, in *CED Cass.*, n. 281501; Cass., sez. VI, sent. 19 gennaio 2021 n. 36420, in *CED Cass.*, n. 281989 – 01).

[25] Cass., sez. I, sent. 19 marzo 2021 n. 12749, in *CED Cass.*, n. 280981 – 01.

[26] Cass., sez. VI, sent. 1 ottobre 2020 n. 28790, in *CED Cass.*, n. 279629; Cass., sez. V, sent. 15 novembre 2016 n. 542, in *CED Cass.*, n. 269020. Sull'inutilizzabilità dei risultati delle intercettazioni si veda, tra gli altri, L. FILIPPI, *Intercettazioni, tabulati e altre limitazioni della segretezza delle comunicazioni*, in G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB (a cura di), *Procedura penale. Teoria e pratica del processo*, I, Milano, 2015, p. 1078.

[27] Cass., sez. V, sent. 28 maggio 2024 n. 34238, in *CED Cass.*, n. 286939; Cass., sez. VI, sent. 07 novembre 2019 n. 1007, in *CED Cass.*, n. 277586 – 01; Cass., sez. I, sent. 30 gennaio 2007 n. 21923, in *CED Cass.*, n. 236694 – 01; in generale, in tema di insussistenza della inutilizzabilità derivata, Cass., sez. V, sent. 27 ottobre 2021 n. 7781,

È stato affermato, infine, che, per stabilire se il "diverso reato" sia connesso rispetto a quello autorizzato, si deve avere riguardo al reato "accertato" per mezzo delle captazioni e non alla mera prospettazione astratta, cioè alla mera possibilità potenziale esistente al momento in cui le intercettazioni sono autorizzate che l'ipotizzato diverso reato sia connesso con quello oggetto della autorizzazione[28]. L'art. 270 c.p.p., infatti, disciplina l'utilizzabilità dei risultati delle intercettazioni e non il diverso profilo della legittimità del provvedimento autorizzativo[29].

Proprio quest'ultima regola lascia emergere un delicato problema operativo che il pubblico ministero deve affrontare: nel corso delle operazioni di intercettazioni, egli deve valutare gli eventuali ulteriori fatti-reato che dovessero emergere, verificando se sussistono ragioni di connessione con quello che è posto a fondamento del provvedimento autorizzativo delle captazioni, optando, in caso di valutazione negativa, per la presentazione di una ulteriore richiesta di autorizzazione che potrebbe riguardare i medesimi interlocutori (e che, per ragioni di opportunità, potrebbe tendenzialmente provare ad allineare sotto il profilo temporale a quella originaria).

Si tratta di una notevole difficoltà operativa che, tuttavia, lascia emergere un importante risvolto del principio espresso dalla sentenza delle Sezioni unite "Cavallo": ripristinando, in forza dei valori costituzionali, uno spazio di azione al divieto di cui all'art. 270 c.p. p., in precedenza trascurato dalla giurisprudenza, è stato imposto al pubblico ministero una precisa modalità per lo svolgimento dell'attività investigativa che si fonda sull'assoluto rispetto dell'art. 268 c.p.p. L'organo pubblico deve seguire i risultati degli ascolti; deve interloquire con la polizia giudiziaria delegata allo svolgimento delle operazioni; non può assolutamente limitarsi ad attendere le informative della polizia giudiziaria perché deve valutare, nel caso molto frequente in cui emergano fatti diversi da quelli che sono stati posti a fondamento del decreto au-

in *CED Cass.*, n. 282898 – 01; Cass., sez. VI, sent. 30 aprile 2019 n. 4119, in *CED Cass.*, n. 278196 – 03.

[28] Cass., sez. V, sent. 13 giugno 2024 n. 40338, in *CED Cass.*, n. 287240.

[29] Cass., sez. VI, sent. 19 gennaio 2021 n. 29194, in *CED Cass.*, 281824 – 01; più di recente, Cass., sez. IV, sent. 20 giugno 2024 n. 33134, inedita; Cass., sez. II, sent. 9 maggio 2023 n. 33350, inedita.

torizzativo, se ricorrono ragioni di connessione che permettono l'utilizzabilità nella prova raccolta, dovendo procedere altrimenti a formulare, se del caso, una nuova richiesta di autorizzazione.

4. La determinazione del "perimetro" dell'autorizzazione del giudice

L'approfondimento della premessa costituzionale della decisione delle Sezioni unite, peraltro, ha segnato il punto di partenza di un successivo percorso di sviluppo della giurisprudenza della Corte di Cassazione.

Dettando una importante regola pratica, è stato evidenziato che il tema dell'utilizzabilità dei risultati delle intercettazioni debba essere affrontato domandandosi, in primo luogo, quale sia il "perimetro" dell'autorizzazione giudiziale rilasciata – ossia, impiegando le parole della sentenza della Corte costituzionale, richiamata dalle Sezioni unite, quali siano cioè «i fatti costituenti reato a essa riconducibili»[30] – per poi successivamente verificare se, in presenza di altri fatti costituenti reato emersi dalle captazioni, sussista o meno quel rapporto di connessione *ex* art. 12 c.p.p. che, unito alla ricorrenza del limite di ammissibilità *ex* art. 266 stesso c.p.p., consente di ravvisare uno "stesso procedimento" e, dunque, di concludere per l'utilizzazione dei relativi risultati.

Per individuare il fatto-reato che ha giustificato il ricorso alle intercettazioni, quindi, non assume rilievo la sua formale iscrizione nel registro delle notizie di reato. Non assume valenza decisiva neppure la circostanza che notizie di reato siano state iscritte nel registro delle notizie di reato in un momento successivo ai provvedimenti autorizzativi le captazioni. Il tema, infatti, attiene non alla legittimità dei provvedimenti autorizzativi, ma piuttosto alla loro utilizzabilità in relazione all'eventuale decorso del termine di durata delle indagini preliminari.

Neppure è rilevante che tale fatto-reato, nella sua originale ipotesi accusatoria, non abbia trovato conferma dai risultati dell'intercettazione o sia stato oggetto di diverso inquadramento giuridico.

[30] C. cost., sent. 11 luglio 1991 n. 366.

Rileva, invece, che tale fatto-reato sia stato oggetto, in senso sostanziale, della richiesta e della prospettazione del pubblico ministero (anche per mezzo di richiamo agli atti di polizia giudiziaria) nonché di una disamina – effettuata anche *per relationem* – dal giudice dell'autorizzazione, compiuta per mezzo di una valutazione del compendio indiziario relativo a tale fatto, del collegamento con l'indagine e con la persona intercettanda[31].

La giurisprudenza, in altri termini, definendo il percorso interpretativo che il giudice deve compiere, ha precisato che ciò che conta è che quel fatto di reato – inteso come un fatto storico necessariamente dotato di specifici elementi indicativi di illiceità, ma prescindendo del tutto da quella che sarà la sua definitiva qualificazione formale e la sua successiva eventuale validazione giudiziale – sia rientrato nel fuoco dell'autorizzazione giudiziale alle captazioni, essendo questo – il legame tra la notizia di fatto-reato e l'autorizzazione alle relative intercettazioni – l'elemento che, secondo l'insegnamento costituzionale esaltato dalle Sezioni unite "Cavallo", consente di giustificare la compressione della libertà e segretezza delle comunicazioni.

Con queste decisioni, dunque, la Corte di Cassazione ha fissato il criterio operativo per il giudice del merito chiamato a valutare il profilo dell'utilizzabilità dei risultati delle intercettazioni. Tale giudice deve confrontarsi con il provvedimento autorizzativo e con le relative eventuali proroghe dello stesso, individuando il fatto-reato che ha permesso le intercettazioni, senza porre particolare rilievo al dato formale dell'iscrizione nel registro delle notizie di reato o alla qualificazione giuridica provvisoriamente assegnata, potendo solo all'esito di tale operazione valutare se il fatto-reato diverso, emerso dagli esiti delle captazioni, sia legato dalla connessione *ex* art. 12 c.p.p. con il precedente che permette di ritenere sussistente uno stesso procedimento.

[31] Cass., sez. VI, sent. 19 gennaio 2021 n. 29194, in *CED Cass.*, n. 281824 – 01; Cass., sez. VI, sent. 19 gennaio 2021 n. 35272, inedita.

5. Segue: la motivazione per relationem *del provvedimento autorizzativo*

La determinazione del "perimetro" dell'autorizzazione alla esecuzione di intercettazioni o alla loro proroga, cioè l'individuazione del fatto-reato di cui è stata ravvisata dal giudice la gravità indiziaria e l'indispensabilità del mezzo di ricerca della prova, è una operazione ermeneutica che può rivelarsi difficile perché va realizzata avendo riguardo non solo alla stessa autorizzazione, ma anche agli atti richiamati e, quindi, pure alla richiesta del pubblico ministero e alle informative di polizia giudiziaria poste a sostegno della stessa.

Secondo l'indirizzo giurisprudenziale consolidato, invero, la motivazione dei decreti autorizzativi delle intercettazioni, nel chiarire le ragioni della sussistenza dei presupposti che legittimano il ricorso a detto intrusivo mezzo di ricerca della prova, deve necessariamente spiegare i motivi che impongono l'intercettazione di una determina utenza telefonica, che fa capo a una specifica persona, indicando la base indiziaria del reato per il quale si procede e il collegamento tra l'indagine in corso e la persona che si intende intercettare, affinché possa esserne verificata, alla luce del complessivo contenuto informativo e argomentativo del provvedimento, l'adeguatezza del mezzo rispetto alla funzione di garanzia prescritta dall'art. 15, co. 2 Cost.[32].

Questa verifica deve essere compiuta al momento in cui la captazione è richiesta e autorizzata, non rilevando, ai fini della utilizzabilità dei risultati dell'attività di intercettazione, la circostanza che, all'esito delle indagini, l'originaria ipotesi accusatoria non sia stata confermata.

La funzione di garanzia assolta dalla motivazione del provvedimento autorizzativo, il fatto cioè che essa debba esplicitare il collegamento tra l'indagine e la persona le cui comunicazioni si intendono intercettare e, più in generale, la sussistenza dei presupposti che legittimano l'adozione del mezzo di ricerca della prova, non esclude che il decreto del giudice possa rinviare ad atti del procedimento, specificamente alla richiesta del pubblico ministero o all'informativa della polizia giudiziaria su cui tale richiesta si fonda.

[32] Cass., sez. VI, sent. 13 giugno 2017 n. 36874, in *CED Cass.*, n. 270814; Cass., sez. VI, sent. 12 febbraio 2009 n. 12722, in *CED Cass.*, n. 243241; Cass., sez. V, sent. 17 novembre 2016 n. 1407, in *CED Cass.*, n. 268900.

Ai fini della legittimità della motivazione *per relationem*, peraltro, è necessario che essa: 1) faccia riferimento, recettizio o di semplice rinvio, a un legittimo atto del procedimento, la cui motivazione risulti congrua rispetto all'esigenza di giustificazione propria del provvedimento di destinazione; 2) fornisca la dimostrazione che il giudice ha preso cognizione del contenuto sostanziale delle ragioni del provvedimento di riferimento e le abbia meditate e ritenute coerenti con la sua decisione; 3) l'atto di riferimento, quando non venga allegato o trascritto nel provvedimento da motivare, sia conosciuto dall'interessato o almeno ostensibile, quanto meno al momento in cui diventi attuale l'esercizio della facoltà di valutazione, di critica ed, eventualmente, di gravame e, conseguentemente, di controllo dell'organo della valutazione o dell'impugnazione[33].

6. La modifica all'art. 270 c.p.p. ad opera della l. 28 febbraio 2020 n. 7 di conversione del d.l. 30 dicembre 2019 n. 161

Immediatamente dopo la sentenza delle Sezioni unite "Cavallo", il legislatore ha modificato l'art. 270, co. 1 c.p.p.[34]. A seguito della riforma, al divieto di utilizzazione dei risultati delle intercettazioni in procedimenti diversi da quelli nei quali sono stati disposti, sono state previste due distinte deroghe. La prima ricalca la disciplina previgente e riguarda l'accertamento dei delitti per i quali è obbligatorio l'arresto in flagran-

[33] Cass., Sez. un., sent. 21 giugno 2000 n. 17, in *CED Cass.*, n. 216664 – 01; Cass., Sez. un., sent. 31 ottobre 2001 n. 42792, in *CED Cass.*, n. 220095.

[34] Su tale normativa si veda anche F. ALVINO, *La circolazione delle intercettazioni e la riformulazione dell'art. 270 c.p.p.: l'incerto pendolarismo tra regola ed eccezione*, cit., 240; A. CAMON, *Art. 270 c.p.p.*, in G. ILLUMINATI, L. GIULIANI (a cura di), *Commentario breve al nuovo codice di procedura penale*, Padova, 2020, p. 1129; D. PRETTI, *La metamorfosi delle intercettazioni, ultimo atto? La legge n. 7/2020 di conversione del d.l. n. 161/2019*, in *Sistema penale* (rivista web), 2 marzo 2020 (ultimo accesso il 28 febbraio 2025); F. CASSIBBA, *In difesa dell'art. 15 Cost.: illegittima la circolazione delle intercettazioni per la prova di reati diversi*, in *Giurisprudenza penale - Rivista trimestrale*, 2020, 2, p. 93 ss.; J. DELLA TORRE, *La nuova disciplina della circolazione del captato: un nodo arduo da sciogliere*, in M. GIALUZ (a cura di), *Le nuove intercettazioni*, in *Diritto di internet*, 2020, *Supplemento* al fascicolo n. 3, p. 90.

za; la seconda concerne i reati di cui all'art. 266, co. 1 c.p.p. («[…] per l'accertamento dei delitti per i quali è obbligatorio l'arresto in flagranza e dei reati di cui all'art. 266, comma 1»).

Per la prova di reati che rientrano nelle suddette deroghe, peraltro, i risultati delle intercettazioni non sono utilizzabili anche in procedimenti diversi da quello in cui sono state autorizzate in modo "automatico", ma solo se sono "rilevanti" e "indispensabili". Al carattere di indispensabilità già previsto, è stato aggiunto quello della rilevanza che pare presupporre una valutazione del "peso" del mezzo di prova nel giudizio[35].

L'utilizzabilità degli esiti delle captazioni realizzate *aliunde*, dunque, dopo la riforma, presuppone che il reato per il quale si procede sia tanto grave che per esso il legislatore ha previsto l'arresto obbligatorio in flagranza oppure che per il titolo di reato accertato sarebbe stato comunque possibile procedere autonomamente a operazioni di intercettazione.

Accanto a questa lettura della norma, secondo cui, nonostante l'utilizzo della congiunzione "e", sarebbe stata disciplinata una doppia deroga al divieto di utilizzazione, è stata anche ipotizzata una interpretazione alternativa alla cui stregua il legislatore richiederebbe, ai fini dell'utilizzabilità delle intercettazioni captate in altro procedimento, che il nuovo delitto in via di accertamento debba essere ricondotto tanto al catalogo dell'art. 380 c.p.p., quanto a quello dell'art. 266 c.p.p.

Il legislatore, comunque, ha recepito solo una delle affermazioni della sentenza delle Sezioni unite "Cavallo", quella secondo cui i risultati delle intercettazioni possono essere utilizzati per la prova dei reati diversi da quelli per i quali sono state disposte soltanto se tali reati sono comunque contenuti nel catalogo di cui all'art. 266, co. 1 c.p.p.

Allontanandosi dai principi delle Sezioni unite, però, è stato previsto che la possibilità di questo utilizzo deriva solo dall'inserimento del rea-

[35] Secondo un indirizzo giurisprudenziale, non è necessario che nel provvedimento che utilizza, ai sensi dell'art. 270 c.p.p., i risultati di intercettazioni effettuate in procedimento diverso sia espressamente motivata l'indispensabilità di tali risultati ai fini dell'accertamento dei delitti per cui si procede e per i quali è previsto l'arresto in flagranza, potendo la valutazione di indispensabilità essere compiuta anche implicitamente, mediante l'attribuzione agli elementi utilizzati di specifica rilevanza ai fini della decisione adottata (Cass., sez. III, sent. 18 gennaio 2022 n. 5821, in *CED Cass.*, n. 282804).

to nel catalogo di cui all'art. 266 c.p.p. (o in quello di cui all'art. 380 c.p.p.) e non dalla unicità del procedimento, desunta nella sentenza delle Sezioni unite dapprima illustrata dall'esistenza di un legame sostanziale tra i diversi fatti-reato.

7. La determinazione dell'area operativa della nuova disposizione

La riforma della disciplina delle intercettazioni disposta con le norme dapprima illustrate si applica, ai sensi dell'art. 9 d.lgs. 29 dicembre 2017 n. 216 e succ. modif. ai «procedimenti penali iscritti dopo il 31 agosto 2020».

Secondo un indirizzo giurisprudenziale, la locuzione «procedimenti penali iscritti dopo il 31 agosto 2020» adoperata dalla disposizione citata, con riguardo alla riforma dell'art. 270 c.p.p., si riferisce ai procedimenti nel cui ambito si intendano utilizzare i risultati di intercettazioni *aliunde* captate e non già ai procedimenti in cui le stesse siano state autorizzate perché

> è solo riguardo la circolazione extraprocedimentale del dato captativo che si pone la questione del divieto di utilizzabilità e delle deroghe, e non già nel diverso procedimento nel quale le intercettazioni stesse siano state generate[36].

Da questa interpretazione dell'art. 9 citato deriva che, qualora il procedimento diverso da quello nel cui ambito le intercettazioni sono state autorizzate sia stato iscritto dopo il 31 agosto 2020, la valutazione di utilizzabilità dei risultati captativi, anche se frutto di attività di indagini compiute prima di tale data, deve essere svolta sulla base dell'art. 270 c.p.p. nella nuova formulazione introdotta dalla riforma, con la conse-

[36] Cass., sez. II, sent. 13 giugno 2023 n. 37143, inedita; Cass., sez. V, sent. 20 luglio 2022 n. 37169, in *CED Cass.*, n. 283874; Cass., sez. V, sent. 20 luglio 2022 n. 37911, inedita. Sul tema, volendo L. GIORDANO, *La Corte di Cassazione sulla disciplina transitoria della riforma delle intercettazioni*, in *Ius penale* (rivista web), 7 febbraio 2022 (ultimo accesso il 28 febbraio 2025); ID., *Intercettazioni: utilizzo in un procedimento diverso ''stralciato'' da quello originario dopo il 31 agosto 2020*, in *Quotidiano Giuridico* (rivista web), 7 settembre 2023 (ultimo accesso il 28 febbraio 2025).

guenza che l'utilizzabilità degli esiti delle captazioni ricorre non solo quando il reato emerso dalle captazioni risulta compreso tra quelli per i quali, ai sensi dell'art. 380 c.p.p., è previsto l'arresto obbligatorio in flagranza, ma anche nel caso in cui detto reato, diverso da quello che ha giustificato le intercettazioni, è ricompreso nel catalogo di cui all'art. 266 c.p.p.

Questo indirizzo giurisprudenziale ha accolto una impostazione che sembra valorizzare il dato letterale della disposizione («procedimenti penali iscritti»), ma anche la *ratio* della norma transitoria. A tale ultimo riguardo, si osserva che il legislatore, intervenendo sulla disposizione transitoria in esame, ha espressamente mutato il parametro temporale per l'applicazione delle nuove norme, in origine fissato al momento della disposizione delle "operazioni di intercettazione", sostituendolo con quello della "iscrizione del procedimento", al fine di

> evitare la commistione di discipline diverse applicabili alle intercettazioni disposte nello stesso procedimento, in tal modo abdicando al principio tempus regit actum, che invece ispirava la precedente versione della stessa disposizione la quale, come si è visto, faceva riferimento all'epoca di adozione dei decreti autorizzativi[37].

L'indirizzo giurisprudenziale illustrato pare ispirarsi anche al principio dell'autonomia di ogni iscrizione. Tale principio, che è stato elaborato ai fini del computo del termine di durata delle indagini preliminari[38], sembra determinare necessariamente l'applicazione delle nuove norme sulle intercettazioni ai procedimenti iscritti dopo il 31 agosto 2020, anche se derivanti dalla separazione di quello originario.

L'art. 335-*quater* c.p.p., del resto, ormai consente l'accertamento della tempestività dell'iscrizione nel registro delle notizie di reato. Pertanto, qualora la persona sottoposta alle indagini ritenga che l'iscrizione (avvenuta a seguito dello "stralcio") della nuova notizia di reato sia in-

[37] Cass., sez. V, sent. 20 luglio 2022 n. 37169, in *CED Cass.*, n. 283874.

[38] Cass., sez. VI, sent. 12 marzo 2003 n. 19053, in *CED Cass.*, n. 227380; Cass., sez. IV, sent. 6 luglio 2006 n. 32776, in *CED Cass.*, n. 234822; Cass., sez. VI, sent. 2 dicembre 2009 n. 11472, in *CED Cass.*, n. 246525; Cass., sez. II, sent. 22 marzo 2013 n. 29143, in *CED Cass.*, n. 256457; Cass., sez. II, sent. 6 marzo 2019 n. 22016, in *CED Cass.*, n. 276965.

tervenuta in ritardo, con conseguente applicazione della nuova versione dell'art. 270 c.p.p. (oppure proprio per permettere l'applicazione della nuova norma), potrebbe chiedere al giudice di accertare la tempestività di tale adempimento, con richiesta di retrodatazione.

Un diverso orientamento giurisprudenziale, invece, ha affermato che la nuova regola contenuta nell'art. 270 c.p.p. non si applica ai risultati delle intercettazioni originariamente disposte in procedimenti iscritti in data anteriore al 31 agosto 2020 (data di efficacia delle modifiche apportate all'art. 270 c.p.p., per effetto dell'art. 9 del d.l. 30 dicembre 2019 n. 161, conv. in l. 28 febbraio 2020 n. 7). A tali intercettazioni, invece, deve essere applicata la precedente disciplina dell'art. 270 c.p.p. che consente l'utilizzazione degli esiti delle captazioni in un procedimento diverso soltanto se indispensabili per l'accertamento di delitti per i quali è previsto l'arresto in flagranza[39].

Secondo questa diversa impostazione, ai fini dell'utilizzabilità degli esiti delle captazioni, non assume rilievo il fatto che, per effetto di sviluppi procedimentali e, dunque, a seguito di separazione da quello originario, dopo il 31 agosto 2020, è stato iscritto un nuovo procedimento, nel quale tuttavia sono confluite le intercettazioni realizzate in precedenza. Infatti,

> le intercettazioni eseguite nella vigenza della precedente disciplina, e quindi disposte nei limiti e alle condizioni stabilite dalle norme di legge vigenti al momento della loro autorizzazione, non possono mutare regime normativo per effetto di sviluppi procedimentali successivi, derivanti dalla decisione di separare dall'originario procedimento alcune posizioni ovvero alcuni reati con conseguente trasmissione degli atti da un ufficio di Procura a un altro, per ragioni di competenza territoriale e/o funzionale[40].

[39] Cass., sez. VI, sent. 11 novembre 2022 n. 4141, inedita; Cass., sez. VI, sent. 24 novembre 2022 n. 9846, in *CED Cass.*, n. 284256.

[40] Cass., sez. VI, sent. 24 novembre 2022 n. 9846, in *CED Cass.*, n. 284256, che richiama anche Cass., sez. VI, sent. 17 novembre 2021 n. 47235, inedita; Cass., sez. VI, sent. 17 novembre 2021 n. 47237, inedita, nelle quali è stato affermato, seppur nelle forme di un sostanziale *obiter dictum*, che la nuova formulazione dell'art. 270 c.p.p. trova applicazione solo con riferimento alle eventuali intercettazioni che fossero eseguite nel procedimento stralciato e oggetto di nuovo iscrizione dopo il 31 agosto 2020.

Secondo questa impostazione, priva di qualsiasi ragionevolezza si rivelerebbe una diversa ricostruzione sistematica, secondo cui le intercettazioni svolte sotto il vigore della pregressa disciplina, nei limiti e alle condizioni stabilite dalle norme di legge vigenti al momento della loro autorizzazione, possano vedere modificato il loro regime per l'effetto retroattivo di vicende processuali successive, afferenti la separazione dei procedimenti e la trasmissione degli atti da un ufficio di procura a un altro, per ragioni di competenza territoriale o funzionale.

Alla stregua di questa seconda impostazione, pertanto, in applicazione dei principi espressi dalla sentenza delle Sezioni unite "Cavallo", gli esiti delle intercettazioni sono utilizzabili anche per l'accertamento di reati diversi da quelli che hanno rappresentato il presupposto del decreto autorizzativo che rientrano nell'elenco di cui all'art. 266 c.p.p., ma solo se è configurabile un procedimento unitario. A tal proposito, però, è necessario che sussista una connessione tra i procedimenti, ai sensi dell'art. 12, co. 1 lett. b) o c) c.p.p.

8. Segue: la sentenza Sezioni unite del 29 aprile 2024, Pisaniello e altri

Il contrasto tra gli indirizzi giurisprudenziali illustrati è stato rimesso alle Sezioni unite[41], chiamate a interpretare il sintagma «procedimenti penali iscritti dopo il 31 agosto 2020» adoperato dall'art. 9 d.lgs. 29 dicembre 2017 n. 216 e successive modificazioni, se riferito al procedimento nell'ambito del quale le intercettazioni sono state disposte ovvero solo al diverso procedimento concernente il reato, non connesso al primo, per l'accertamento del quale le intercettazioni risultano rilevanti e indispensabili.

Le Sezioni unite hanno ritenuto che la disciplina del regime di utilizzabilità delle intercettazioni in procedimenti diversi, di cui all'art. 270, co. 1 c.p.p. – nel testo introdotto dal d.l. 30 dicembre 2019 n. 161, convertito, con modificazioni, dalla l. 28 febbraio 2020 n. 7 e anteriore al d.l. 10 agosto 2023 n. 105, convertito, con modificazioni, dalla l. 8 ot-

[41] Cass., sez. V, ord. 14 novembre 2023 n. 46832, in *Giur. it.*, 2024, p. 1442, con nota di G. QUAGLIANO, *Le Sezioni unite chiamate a pronunciarsi sul 270 c.p.p.: vecchi problemi e nuove norme*.

tobre 2023 n. 137 – si applica solo nel caso in cui il procedimento nel quale sono state compiute le intercettazioni sia stato iscritto successivamente al 31 agosto 2020.

La Corte di legittimità ha ritenuto che tale soluzione interpretativa, oltre che fondata sul dato letterale, sia "costituzionalmente orientata". Le indicazioni offerte dalla giurisprudenza costituzionale, infatti, se non consentono di dubitare della conformità ai precetti costituzionali delle deroghe al divieto di utilizzazione dei risultati delle intercettazioni in procedimento diverso operato dal legislatore del 2019, in quanto non irragionevole, certamente impongono di delimitare l'ambito di estensione temporale della disposizione in esame in modo tale da evitare che essa trovi applicazione con riferimento a intercettazioni compiute sotto l'egida della vecchia disciplina, dunque disposte nei limiti e alle condizioni stabilite dalle norme di legge vigenti al momento della loro autorizzazione[42].

9. La nuova riforma dell'art. 270 c.p.p. intervenuta nel 2023

La l. 9 ottobre 2023 n. 137 di conversione del d.l. 10 agosto 2023 n. 105, in seguito, è intervenuta nuovamente sulla disciplina dell'utilizzazione dei risultati delle intercettazioni in procedimenti diversi da quelli in cui il mezzo di ricerca della prova è stato disposto[43].

L'art. 1, co. 2-*quater*, citato, infatti, ha riformato l'art. 270, co. 1 c.p.p., sopprimendo le parole «e dei reati di cui all'articolo 266, comma 1». È stata eliminata, pertanto, proprio quella parte della disposizio-

[42] L'interpretazione della norma transitoria accolta, inoltre, evita di estendere o restringere la possibilità di utilizzare gli esiti delle captazioni in procedimenti diversi sulla base di valutazioni variabili in base a scelte dell'organo della pubblica accusa.

[43] Sulla nuova riforma, tra gli altri, A. CELOTTO, *Sulla conversione in legge del decreto-legge 10 agosto 2023*, n. 105, in *Giurisprudenza penale* (rivista web), 13 settembre 2023 (ultimo accesso il 28 febbraio 2025); L. FILIPPI, *La miniriforma delle intercettazioni: più luci che ombre*, in *Penale diritto e procedura* (rivista web), 19 ottobre 2023 (ultimo accesso il 28 febbraio 2025); G.L. GATTA, *Intercettazioni e criminalità organizzata: quando a voler precisare si finisce per complicare*, in *Sistema penale* (rivista web), 8 agosto 2023 (ultimo accesso il 28 febbraio 2025); volendo, L. GIORDANO, *Una nuova riforma della disciplina delle intercettazioni*, in *Dir. pen. proc.*, 2024, p. 11.

ne che era stata inserita nell'art. 270, co. 1 c.p.p. dall'art. 2, co. 1 lett. g), del d.l. n. 161 del 2019. Di conseguenza, per l'utilizzo in procedimenti diversi dei risultati delle intercettazioni effettuate altrove, non basta più che il reato emerso rientri nel catalogo di quelli che, ai sensi dell'art. 266 c.p.p., permettono l'uso delle intercettazioni. L'uso dei risultati delle intercettazioni svolte in un diverso procedimento, invece, presuppone che gli ascolti siano rilevanti e indispensabili per l'accertamento dei delitti per i quali è obbligatorio l'arresto in flagranza. Con la riforma, pertanto, è stata riproposta la disciplina precedente.

È stata prevista, poi, una disciplina transitoria. In deroga al principio *tempus regit actum*, è stato stabilito, all'art. 1, co. 2-*quinquies* del d.l. cit., che «la disposizione di cui al comma 2-*quater* si applica ai procedimenti iscritti successivamente alla data di entrata in vigore della legge di conversione del presente decreto», entrata in vigore avvenuta il 10 ottobre 2023, proponendo una formulazione che richiama quella adottata dall'art. 9 d.lgs. n. 216 del 2017 in occasione della riforma complessiva della disciplina delle intercettazioni.

In applicazione del principio espresso dalle Sezioni unite sembrerebbe doversi ritenere che la nuova disciplina dell'art. 270 c.p.p. operi soltanto nel caso in cui entrambi i procedimenti, quello nel quale sono state compiute le intercettazioni e quello nel quale si intendano utilizzare i risultati delle captazioni, siano stati iscritti dopo il 10 ottobre 2023.

10. Il deposito di verbali e registrazioni nel procedimento diverso

Secondo l'indirizzo giurisprudenziale consolidato, ai fini dell'utilizzabilità degli esiti di intercettazioni di conversazioni o comunicazioni in procedimento diverso da quello nel quale esse sono state disposte, non occorre la produzione del relativo decreto autorizzativo, essendo sufficiente il deposito, presso l'autorità giudiziaria competente per il "diverso" procedimento, dei verbali e delle registrazioni delle intercettazioni medesime[44].

[44] Cass., Sez. un., sent. 17 novembre 2004 n. 45189, in *CED Cass.*, n. 229244 – 01.

Secondo l'art. 270, co. 2 c.p.p., infatti, ai fini dell'utilizzazione prevista dal comma precedente sono depositati presso l'autorità competente per il diverso procedimento i verbali e le registrazioni delle intercettazioni.

La nuova legge non è intervenuta su questo profilo della disciplina dell'utilizzazione dei risultati delle intercettazioni in un procedimento diverso. Si tratta di un aspetto che incide in modo rilevante sulla possibilità di controllo della legittimità del decreto autorizzativo originario[45].

La Corte di Cassazione, difatti, ha avuto modo di precisare che l'omesso deposito del decreto autorizzativo non ne determina l'inutilizzabilità, neanche a seguito delle modifiche introdotte dalla l. 9 ottobre 2023 n. 137, posto che l'art. 270, co. 2 c.p.p. continua a prevedere il solo deposito, presso l'autorità giudiziaria competente per il procedimento diverso da quello nel quale l'attività captativa è stata disposta, delle registrazioni e dei verbali delle intercettazioni da utilizzare[46].

Colui che intendesse far valere la illegittimità del decreto autorizzativo, pertanto, deve chiederne copia nell'originario procedimento in cui il decreto è stato adottato e, successivamente, depositare tale copia nel diverso procedimento a sostegno della eccezione di illegittimità dell'atto[47].

Sul punto, va evidenziato che l'art. 2 l. 9 agosto 2024 n. 114, modificando diverse norme del codice di procedura penale e riformando al-

---

[45] Sul tema E.N. LA ROCCA, *L'uso dei risultati delle intercettazioni in procedimenti diversi*, in P. MAGGIO (a cura di), *La nuova disciplina delle intercettazioni*, Torino, 2023, p. 399.

[46] Cass., sez. I, sent. 14 novembre 2023 n. 49627, in *CED Cass.*, n. 285579 – 02.

[47] Grava sulla parte, che eccepisce l'invalidità o l'inutilizzabilità delle intercettazioni provenienti da altro procedimento, l'onere di allegare e provare il fatto dal quale dipende la patologia denunciata (Cass., Sez. un., sent. 17 novembre 2004 n. 45189, cit.), e, quindi, nel caso di censura concernente il vizio di motivazione apparente, di produrre sia il decreto di autorizzazione emesso nel procedimento diverso, sia il documento al quale esso rinvia (Cass., Sez. un., sent. 17 novembre 2004 n. 45189, cit.; Cass, sez. I, sent. 18 febbraio 2019 n. 11168, in *CED Cass.*, n. 274996). È stato sostenuto che, ai sensi dell'art. 116 c.p.p., l'interessato non sia titolare di un diritto potestativo al rilascio di copie, ma della sola possibilità di tale rilascio, potendo vedersi opporre un diniego, motivato per esempio con la necessità di salvaguardare la segretezza delle indagini, che sarebbe inoppugnabile e che precluderebbe l'accertamento dell'illegalità della prova (cfr. E.N. LA ROCCA, *L'uso dei risultati delle intercettazioni in procedimenti diversi*, cit., p. 401).

cune disposizioni che disciplinano le intercettazioni di conversazioni o comunicazioni, ha inserito nell'art. 116, co. 1 c.p.p. un ulteriore periodo che è volto ad assicurare efficacia al divieto di pubblicazione illustrato. In forza della nuova norma, infatti, è stato escluso il rilascio di «copia delle intercettazioni di cui è vietata la pubblicazione ai sensi dell'art. 114 co. 2-*bis*, c.p.p., quando la richiesta è presentata da un soggetto diverso dalle parti e dai loro difensori». La richiesta di copia, però, può essere accolta se «sia motivata dalla esigenza di utilizzare i risultati delle intercettazioni in altro procedimento specificamente indicato».

A discapito della riservatezza dei titolari delle utenze intercettate non pubblicabili, dunque, oltre all'interesse a conoscere le captazioni di natura processuale facente capo a chi sia parte nel procedimento, è garantito soltanto quello di chi intenda utilizzare gli esiti dell'intercettazione in un altro procedimento che va specificato.

Per mera completezza, va segnalato che, secondo un indirizzo giurisprudenziale, nella diversa fattispecie in cui il contenuto di una captazione costituisca il presupposto di nuove e autonome intercettazioni disposte in un diverso procedimento, per l'utilizzabilità degli esiti di queste ultime non occorre il deposito dei decreti autorizzativi del procedimento *a quo*, le cui risultanze influiscono sulle autorizzazioni relative al procedimento *ad quem* come mero presupposto di fatto, incidente sulla motivazione dei successivi, autonomi decreti solo sotto il profilo della loro rilevanza ai fini della verifica dei "gravi indizi di reato", richiesta dall'art. 267, co. 1 c.p.p.[48].

11. Il particolare regime della circolazione dei risultati delle intercettazioni realizzate tramite trojan

L'art. 270, co. 1-*bis* c.p.p. disciplina l'utilizzo dei risultati delle intercettazioni tra presenti operate con captatore informatico per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione è una disposizione di non agevole interpretazione, stabilendo che

[48] Cass., sez. V, sent. 27 ottobre 2021 n. 7781, Cordua, in *CED Cass.*, n. 282898.

> fermo restando quanto previsto dal comma 1, i risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione qualora risultino indispensabili per l'accertamento dei delitti indicati dall'articolo 266, comma 2-*bis*[49].

Secondo una interpretazione, la norma in esame, pur formulata in positivo, fissa la regola del divieto di uso dei risultati delle intercettazioni per la prova di reati diversi da quelli per cui sono state disposte,

[49] Per una completa ricostruzione del tema, si veda M. ANTINUCCI, G. SPANGHER, *Davvero possibili le intercettazioni c.d. a strascico attraverso l'uso del captatore informatico per reati comuni?*, in *Dir. pen. proc.*, 2020, p. 1128; G. SANTALUCIA, *Il diritto alla riservatezza nella nuova disciplina delle intercettazioni*, in *Sistema penale*, 2020, 1, p. 58; P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in G. GIOSTRA, R. ORLANDI (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, p. 257; W. NOCERINO, *Il captatore informatico: un giano bifronte. Prassi operative vs risvolti giuridici*, in *Cass. pen.*, 2020, p. 831. Sia consentito il rinvio anche a L. GIORDANO, *La disciplina della circolazione dei risultati delle captazioni compiute tramite "trojan"*, in *Ius penale* (rivista web), 22 agosto 2022 (ultimo accesso il 28 febbraio 2025). Sulla disciplina del captatore, tra i numerosi contributi, si segnalano S. ATERNO, *Digital forensics (investigazioni informatiche)*, in *Digesto Pen.*, Agg., VIII, Torino, 2014, p. 217; R. FLOR, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di internet*, in *Diritto penale contemporaneo* (rivista web), 22 settembre 2012 (ultimo accesso il 28 febbraio 2025); F. IOVENE, *Le c.d. perquisizioni* on line*: tra nuovi diritti fondamentali ed esigenze di accertamento penale*, *ivi*, 27 febbraio 2014 (ultimo accesso il 28 febbraio 2025); A. LORENZETTO, *Il perimetro delle intercettazioni ambientali eseguite mediante "captatore informatico"*, *ivi*, 24 marzo 2016 (ultimo accesso il 28 febbraio 2025); S. MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in *Cass. pen.*, 2010, p. 2855; ID., *Le indagini atipiche a contenuto tecnologico nel processo penale: Una proposta*, *ivi*, 2015, p. 760 ss.; L. PALMIERI, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza "Scurato" alla riforma sulle intercettazioni*, in *Diritto penale contemporaneo - Rivista trimestrale*, 2018, 1, p. 59 ss.; A. TESTAGUZZA, *I sistemi di controllo remoto: tra normativa e prassi*, in *Dir. pen. proc.*, 2014, p. 759; M. TORRE, *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, *ivi*, 2015, p. 1163; M. TROGU, *Le intercettazioni di comunicazioni a mezzo Skype*, in *Processo penale e giustizia*, 2014, 3, p. 102.

stabilendo anche la deroga a tale divieto nel caso in cui le captazioni servano «per l'accertamento dei delitti indicati dall'art. 266, comma 2-bis».

Tale deroga, inoltre, è condizionata alla indispensabilità probatoria degli esiti di tali captazioni.

Il divieto di utilizzo degli esiti delle captazioni, più precisamente, presenta un'area operativa più ampia rispetto a quella disegnata dall'art. 270, co. 1 c.p.p.: infatti, esso non riguarda l'utilizzo dei risultati delle intercettazioni per la prova dei reati emersi in "procedimenti diversi", ma l'impiego di tali risultati per la prova di "reati diversi" da quello per cui è stata autorizzata l'intercettazione dal Gip.

Il divieto, pertanto, opera anche nell'ambito dello stesso procedimento, cioè quando tra il fatto-reato per il quale le intercettazioni sono state disposte dal giudice e quello emerso dalle captazioni sussistano quelle ragioni di connessione – quel legame sostanziale forte – che, come è stato chiarito dalla sentenza delle Sezioni unite "Cavallo", permettono di ravvisare l'unicità del procedimento.

Proprio la necessità di escludere il rilievo probatorio degli esiti delle captazioni anche nell'ambito del medesimo procedimento avrebbe determinato la differente formulazione della norma in esame rispetto a quanto già previsto dal comma 1 dello stesso art. 270 c.p.p.

Anche la deroga al divieto di utilizzo dei risultati delle captazioni, inoltre, è più circoscritta rispetto alla deroga al divieto previsto dal comma primo della medesima norma: non vale per tutti i reati di cui all'art. 380 c.p.p. per i quali è obbligatorio l'arresto in flagranza, come è attualmente previsto dall'art. 270, co. 1 c.p.p., ma solo per i delitti per i quali, ai sensi dell'art. 266, co. 2-*bis* c.p.p., è sempre consentito l'impiego del *trojan* nelle indagini.

La clausola di salvezza con cui si apre la norma («fermo restando quanto previsto dal comma 1»), secondo questa impostazione, servirebbe solo a rimarcare che, a differenza di quanto previsto dall'art. 270, co. 1 c.p.p., nel caso in cui per realizzare le intercettazioni si è usato il captatore informatico, il divieto di utilizzazione dei risultati presenta una più ampia portata e una deroga più limitata.

Questa soluzione è stata accolta dalla Corte di Cassazione[50].

In detta decisione, peraltro, è stato precisato che il divieto di utilizzazione dei risultati delle intercettazioni realizzate tramite *trojan* per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione e la limitata deroga disciplinata dalla stessa norma per l'accertamento dei delitti indicati dall'art. 266, co. 2-*bis* c.p.p. sono relativi ai soli risultati delle intercettazioni tra presenti.

Secondo la sentenza, pertanto, qualora con il captatore informatico fossero state registrate "chiamate vocali" oppure fossero state acquisite "chat" o "messaggi istantanei", tali esiti delle intercettazioni sarebbero utilizzabili anche in procedimenti diversi ai sensi dell'art. 270, co. 1 c.p.p. a condizione che siano rilevanti e indispensabili per l'accertamento di delitti per i quali è previsto l'arresto obbligatorio in flagranza. Quest'ultimo, secondo la Corte di Cassazione, è il significato da attribuirsi all'inciso di non facile interpretazione con cui si apre l'art. 270, co. 1-*bis*, c.p.p. («fermo restando quanto previsto dal comma 1»).

L'interpretazione dell'art. 270, co. 1-*bis* c.p.p. accolta dalla sentenza illustrata, peraltro, suscita dubbi sulla ragionevolezza di una norma che prevede una distinzione, ai fini dell'utilizzabilità dei risultati delle intercettazioni, in base allo strumento tecnico utilizzato per realizzarle. Nei confronti di un indagato per lo stesso reato, anche nello stesso procedimento, cioè per fatti connessi e per i quali autonomamente potevano essere disposte intercettazioni, gli esiti delle intercettazioni potrebbero essere usati come prova se compiuti con mezzi tradizionali e sarebbero inutilizzabili se le captazioni sono state realizzate con il *trojan*.

L'art. 266, co. 2 c.p.p., tuttavia, dispone che l'intercettazione tra presenti «può essere realizzata anche tramite captatore informatico», lasciando intendere, come hanno riconosciuto di recente anche le Sezioni unite nella sent. 29 febbraio 2024 n. 23756 che si è occupata delle *chat* tratte dai c.d. criptofonini, che il captatore informatico costituisca solo lo strumento tecnico impiegato per realizzare le intercettazioni.

La Corte di Cassazione, tuttavia, nella sentenza citata in precedenza non ha accolto l'istanza della Procura generale che ha chiesto di solle-

[50] Cass., sez. IV, sent. 20 giugno 2024 n. 25401, in *CED Cass.*, n. 286472, in *Ius penale* (rivista web), 4 luglio 2024, con nota di L. GIORDANO, *La circolazione delle intercettazioni effettuate con il trojan* (ultimo accesso il 28 febbraio 2025).

vare questione di legittimità costituzionale, ritenendo giustificata la diversità di disciplina illustrata.

*12. Segue: una diversa interpretazione dell'art. 270, co. 1-*bis *c.p.p.*

Secondo una diversa interpretazione, l'intera disciplina dell'art. 270 c.p.p., anche quella contenuta nel comma 1-*bis*, riguarda l'uso degli esiti delle intercettazioni in "altri procedimenti", come risulta dal titolo della disposizione. Solo nell'ambito di procedimenti diversi – cioè, secondo la lettura dell'art. 270 c.p.p. accolta dalle Sezioni unite della Corte di Cassazione nella sentenza "Cavallo", nel caso di emersione dalle captazioni di fatti-reato non connessi con quelli per i quali è stata disposta l'intercettazione – opererebbe il divieto di utilizzo probatorio dei risultati, salvo che si tratti di reati per i quali il ricorso al captatore, ai sensi dell'art. 266, co. 2-*bis* c.p.p., "è sempre consentito". Nell'ambito dello stesso procedimento, invece, cioè quando ricorre tra il reato che ha giustificato l'intercettazione e quello emerso dalle captazioni una ragione di connessione *ex* art. 12 c.p.p., deve trovare applicazione la regola generale che presuppone, per l'utilizzo dei risultati delle captazioni, che il reato emerso rientri nel catalogo dell'art. 266 c.p.p. Nello stesso procedimento, dunque, basterebbe per l'uso degli esiti delle intercettazioni – anche di quelle realizzate con il *trojan* – che il reato accertato rientri tra quelli per i quali è legittimo l'uso delle intercettazioni.

L'ACQUISIZIONE TRANSFRONTALIERA DI PROVE DIGITALI

Rosanna Belfiore

SOMMARIO: *1. La fisionomia della prova digitale: brevi cenni. 2. L'acquisizione della prova digitale nell'Unione europea. 2.1. L'ordine europeo di indagine penale. 2.1.1. La questione della garanzia giurisdizionale. 2.1.2. La questione dell'utilizzabilità della prova. 2.2. La Procura europea. 2.3. L'ordine europeo di produzione e conservazione di prove elettroniche.*

1. La fisionomia della prova digitale: brevi cenni

L'acquisizione di prove digitali attiene all'approvvigionamento di dati e informazioni presenti all'interno di sistemi informatici, sia su supporti fisici che in rete, utilizzabili per provare un fatto in un procedimento penale. Si tratta di dati e informazioni conservati nei *device* ovvero dai fornitori di servizi, ma anche di flussi informativi e di corrispondenza elettronica[1].

A connotare la prova digitale sono, dunque, l'immaterialità e l'ubiquità. Siamo, cioè, di fronte a una prova intangibile perché esistente a prescindere dal suo supporto e replicabile perché trasferibile su altri supporti, potendosi trovare nello stesso momento all'interno di più dispositivi. In quanto tale, la prova digitale è precaria, volatile perché facilmente alterabile, sovrascrivibile o cancellabile[2]. Non solo. La prova

[1] Corrispondenza che, almeno nella dimensione interna, continua a essere tale «anche dopo la ricezione da parte del destinatario, almeno fino a quando […] non abbia perso ogni carattere di attualità […] trasformandosi in mero documento storico», come ha stabilito C. cost., sent. 27 luglio 2023, n. 170.

[2] In argomento v. per tutti: G. DI PAOLO, voce *Prova informatica (diritto processuale penale)*, in *Enc. dir., Annali*, VI, Milano, 2013, p. 736 ss. Sotto altro aspetto, attinente specificatamente alle indagini digitali, v. S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018.

digitale è anche transnazionale per natura[3], ossia slegata da una precisa giurisdizione, o perché non collocabile in un certo territorio se non virtualmente (pensiamo ai dati in rete), o perché comunque accessibile autonomamente da remoto e quindi da ogni luogo. In questi termini, la prova digitale è tale da scardinare le note categorie di sovranità, territorialità e giurisdizione[4], e, nell'ottica della cooperazione transfrontaliera, le altrettanto note categorie di *lex loci* e *lex fori*, che valgono di norma a preservare la giurisdizione da elementi probatori spuri[5].

In questo quadro in cui la prova digitale travalica i tradizionali confini nazionali, sembra quasi che l'assistenza giudiziaria transfrontaliera sia ormai superflua. E invece la cooperazione continua a essere necessaria: o perché l'attività acquisitiva della prova digitale richiede l'assistenza tecnica di un altro Stato ovvero un'apposita notifica (tipico è il caso delle intercettazioni di flussi comunicativi); o perché la prova digitale è stata già acquisita da uno Stato di propria iniziativa nell'ambito di altra indagine; o perché i dati di interesse sono detenuti da un *service provider* straniero. Per ognuno di questi casi, vi è uno strumento di cooperazione – non sempre *ad hoc* per la verità – dalla cui applicazione discendono una serie di problemi, che la giurisprudenza (sovranazionale e domestica) si trova oggi ad affrontare.

---

[3] Così F. SIRACUSANO, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *Processo penale e giustizia*, 2017, p. 178 (nell'*abstract*). Analog., v. M.A. BIASIOTTI, S. CONTI, F. TURCHI, *La raccolta transnazionale della prova digitale in ambito europeo: una proposta per l'adozione di uno* standard, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), Cybercrime. *Diritto e Procedura Penale dell'Informatica*, Milano, 2019, p. 1641 s.

[4] Così, ancora, F. SIRACUSANO, *op. cit.*, p. 181. In una prospettiva più ampia, sottolinea S. LORUSSO, *La sfida dell'intelligenza artificiale al processo penale nell'era digitale*, in *Sistema penale* (rivista web), 28 marzo 2024, p. 2 (ultimo accesso il 28 febbraio 2025) che, con la rivoluzione digitale, «[…] ad essere sgretolata è la fondamentale unità spazio-temporale che caratterizza da sempre l'esercizio della giurisdizione penale […] la dimensione fisica (il "dove") diviene meramente eventuale e, se del caso, virtuale».

[5] Sul punto, v. G. DALIA, *La natura transnazionale della* digital evidence *tra richieste di cooperazione e pretese di sovranità*, in *Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, 2023, 1, p. 38.

2. L'acquisizione della prova digitale nell'Unione europea

Per ragioni di concentrazione, ci si soffermerà solo sugli strumenti a disposizione nel quadro della cooperazione giudiziaria nell'Unione europea, trattandosi di una dimensione all'avanguardia rispetto a quella della cooperazione propriamente internazionale, in cui pure opera – va detto – l'importante Convenzione di Budapest sulla criminalità informatica del 2001; non opera, invece, il II Protocollo addizionale sulla cooperazione rafforzata e la divulgazione di prove elettroniche, firmato a Strasburgo il 12 maggio 2022 e ancora in corso di ratifica[6]. Un Protocollo, peraltro, promosso dagli organismi eurounitari che, con la decisione 2023/436, hanno autorizzato gli Stati membri a ratificarlo, proprio nell'interesse dell'Unione[7].

2.1. L'ordine europeo di indagine penale

Nella dimensione eurounitaria, il trasferimento della prova digitale può avvenire, innanzitutto, mediante la misura di assistenza giudiziaria per eccellenza, fondata sull'ormai ben assestato principio di mutuo riconoscimento. Il riferimento è, evidentemente, all'ordine europeo di indagine, che, sebbene non si occupi specificatamente della prova elettronica, è stato di recente protagonista di un'importante sentenza della grande sezione della Corte di giustizia dell'Unione europea[8] (d'ora in poi "la Corte"), chiamata – dal Tribunale di Berlino – a confrontarsi proprio con il trasferimento di prove digitali, consistenti in un'enorme mole di dati relativi a comunicazioni (prevalentemente messaggistica) avvenute tramite telefoni cellulari criptati funzionanti con la licenza

[6] Il II Protocollo è stato firmato da 44 Stati e ratificato a oggi solo da 2. Per un approfondimento sul contenuto di questo Protocollo, v. G. DALIA, *op. cit.*, p. 41 ss.

[7] Si tratta della Decisione (UE) 2023/436 del Consiglio del 14 febbraio 2023 che autorizza gli Stati membri a ratificare, nell'interesse dell'Unione europea, il secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche.

[8] CGUE, grande sezione, sent. 30 aprile 2024, causa C-670/22, M.N. Per un approfondimento sulla vicenda giudiziaria e sul contenuto della sentenza, sia consentito rinviare a R. BELFIORE, *L'ordine europeo di indagine nella sentenza "Encrochat" della Corte di giustizia UE*, in *Riv. it. dir. proc. pen.*, 2024, p. 1264 ss.

"EncroChat" e non intercettabili con metodi di indagine tradizionali[9]. Questi dati sono stati raccolti dalle autorità francesi, nell'ambito di un'indagine condotta da una squadra investigativa comune con i Paesi Bassi, grazie a un *software* di tipo "Trojan", caricato, previa autorizzazione giurisdizionale, su un *server* installato nel territorio francese e da lì sui telefoni cellulari criptati tramite un aggiornamento simulato, che avrebbe interessato 32.477 utenti su un totale di 66.134 utenti iscritti, 4.600 dei quali in Germania. Le autorità tedesche – tra le altre – erano state informate della misura di intercettazione dei criptofonini in occasione di una videoconferenza appositamente organizzata da Eurojust, a seguito della quale la procura generale di Francoforte aveva dapprima avviato un'inchiesta e poi emesso tre ordini europei di indagine per ottenere i dati dei telefoni cellulari di utenti tedeschi dotati del servizio "EncroChat" e in possesso delle autorità francesi.

2.1.1. La questione della garanzia giurisdizionale

La prima questione sollevata dal giudice tedesco riguarda l'individuazione dell'autorità competente a emettere un ordine europeo volto all'acquisizione di prove già in possesso dello Stato di esecuzione, quando la raccolta iniziale di tali prove avrebbe dovuto essere ordinata da un giudice in forza del diritto interno, e sia stata effettuata nel territorio dello Stato di emissione nei confronti di un gruppo indiscriminato di utenti aventi in uso telefoni cellulari che permettono una comunicazione cifrata. Il Tribunale di Berlino dubita, infatti, che alla luce della direttiva 2014/41/UE siano legittimi gli ordini europei emessi dalla procura per ottenere i risultati di intercettazioni, suscettibili a norma del diritto tedesco di essere ordinate solo da un giudice, ed effettuate dalle autorità francesi su utenze criptate in Germania indipendentemente dal-

[9] Sul 'caso Encrochat' v.: G. DI PAOLO, *La circolazione transfrontaliera delle prove elettroniche*, in *Penale Diritto e Procedura* (rivista web), 13 maggio 2024, p. 2 s. (ultimo accesso il 28 febbraio 2025); e J.J. OERLEMANS, D. VAN TOOR, *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2022, p. 309 ss. Sul funzionamento delle piattaforme crittografate sotto il profilo tecnico, v. O. MURRO, *Lo* smartphone *come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati*, Milano, 2024, p. 20 ss.

l'esistenza di una presunzione di reato grave fondata su fatti concreti a carico di ciascuna persona interessata. I dubbi di legittimità sono stati ulteriormente alimentati dall'insondabilità circa l'integrità del dato probatorio trasmesso, a causa del segreto militare opposto dalle autorità francesi.

Un primo profilo concerne, quindi, la rilevanza della garanzia della giurisdizione rispetto a richieste di prove già raccolte, cui la Corte dà riscontro richiamando senza indugio gli artt. 1.1 e 2, lett. c), i) della direttiva 2014/41, là dove il pubblico ministero figura espressamente tra le «autorità di emissione»[10], purché competente nel caso concreto. Qualora un pubblico ministero sia competente in un caso puramente interno a ordinare la trasmissione di prove già in possesso delle autorità nazionali, quest'ultimo rientra nella nozione di «autorità di emissione» ai fini di un ordine europeo diretto alla trasmissione di prove già in possesso dello Stato di esecuzione[11]. La Corte esprime così un principio condivisibile, cui peraltro si è uniformata la nostra Corte di Cassazione nel noto caso Sky-ECC[12]: occorre dare rilievo al diritto dello Stato di emissione sia quando l'assistenza giudiziaria riguardi le prove costituende, da acquisire su specifica richiesta, sia quando l'assistenza giudiziaria riguardi le prove precostituite, acquisite *motu proprio* dall'autorità di

[10] In CGUE, grande sezione, sent. 8 dicembre 2020, causa C-584/19, A. e a., la Corte ha anzi avuto modo di chiarire che rientra nelle nozioni di «autorità giudiziaria» e di «autorità di emissione» ai fini dell'adozione di un ordine europeo d'indagine, il pubblico ministero di uno Stato, indipendentemente dal suo eventuale rapporto di subordinazione con il potere esecutivo e dalla sua possibile esposizione al rischio di essere soggetto, direttamente o indirettamente, a ordini o istruzioni da parte del predetto potere. Diversamente, in CGUE, grande sezione, sent. 27 maggio 2019, cause C-508/18 e C-82/19, O.G. e P.I., la Corte ha elaborato una nozione autonoma di «autorità giudiziaria emittente» ai fini dell'adozione di un mandato d'arresto europeo – in assenza di una definizione nella relativa decisione quadro 2002/584/GAI –, incentrata sul necessario requisito di indipendenza dal potere esecutivo.

[11] In linea con CGUE, sent. del 16 dicembre 2021, causa C-724/19, H.P.

[12] Cfr. Cass., sez. un., sent. 29 febbraio 2024, n. 23755, Gjuzi, e Cass., sez. un., sent. 29 febbraio 2024, n. 23756, Giorgi e a., entrambe in *Cass. pen.*, 2024, p. 2553 e p. 2575: in materia di ordine europeo di indagine, le prove già in possesso delle autorità competenti dello Stato di esecuzione possono essere legittimamente richieste ed acquisite dal pubblico ministero italiano senza la necessità di preventiva autorizzazione da parte del giudice del procedimento nel quale si intende utilizzarle.

esecuzione. Se la trasmissione tra procedimenti domestici di prove già acquisite è consentita dal diritto nazionale su iniziativa del pubblico ministero, su sua iniziativa deve essere consentita altresì la trasmissione transfrontaliera dello stesso tipo di prove. Poi, che la circolazione di prove tra procedimenti sia discutibile sul piano di principi fondamentali del processo – *a fortiori* quando si tratti di circolazione di risultati di intercettazioni tra procedimenti stranieri – è un'osservazione certamente non trascurabile[13], su cui si tornerà a breve.

D'altra parte, non vi è dubbio che nel caso di specie si tratti di circolazione di risultati di intercettazioni poiché non vi è dubbio che rientri nella nozione di intercettazioni di telecomunicazioni ai sensi dell'art. 31 della direttiva 2014/41 la misura adottata dalle autorità francesi, consistente nell'infiltrazione in apparecchi terminali diretta a estrarre dati relativi al traffico, all'ubicazione e alle comunicazioni di un servizio di comunicazione basato su Internet – perciò da notificarsi all'autorità designata nello Stato dell'intercettato, a tutela sia della sovranità nazionale che dei diritti delle persone interessate –. Lo stabilisce la Corte, senza troppi distinguo, sulla base di un'interpretazione autonoma della nozione di intercettazioni, adottata in assenza di un rinvio al diritto degli Stati membri e a garanzia dell'uniformità del diritto dell'Unione.

L'altro profilo enucleato dal giudice del rinvio, strettamente collegato al primo, concerne le condizioni per l'emissione di un ordine europeo diretto all'acquisizione di prove già in possesso dell'autorità di esecuzione. Il tribunale tedesco chiede cioè: se, a norma della direttiva, sia necessaria la sussistenza di gravi indizi di colpevolezza a carico di ciascuno dei soggetti interessati; se, sempre a norma della direttiva, sia necessaria la previa verifica dell'integrità dei dati richiesti; e se, ancora a norma della direttiva, sia necessario che l'emissione dell'ordine soddisfi le condizioni per l'acquisizione delle prove anche quando finalizzato a ottenere prove già raccolte.

La Corte richiama subito l'art. 6.1 della direttiva 2014/41, là dove si richiede all'autorità di emissione di effettuare tanto un vaglio di necessità e proporzionalità dell'ordine europeo rispetto al procedimento in

[13] Per simili considerazioni sia consentito rinviare a R. BELFIORE, *Immediatezza e prova transnazionale*, in *Cass. pen.*, 2021, p. 2197.

corso tenendo conto dei diritti della persona indagata o imputata, quanto un vaglio di conformità dell'atto di indagine richiesto alle condizioni previste dal proprio diritto nazionale. Il fine è evidentemente duplice: circoscrivere l'uso dello strumento eurounitario ai soli reati di una certa gravità ed evitare l'elusione delle condizioni di legge previste nello Stato di emissione. Orbene – stando a quanto affermato dalla Corte e ripreso dalla Corte di Cassazione nel menzionato caso Sky-ECC[14] –, poiché questi vagli devono essere effettuati unicamente alla luce del diritto dello Stato di emissione, non è l'art. 6.1 *ex se* – ma può semmai essere il diritto nazionale – a subordinare, sotto il profilo della necessità e proporzionalità, l'emissione di un ordine europeo all'esistenza di una presunzione di reato grave fondata su fatti concreti a carico di ciascuna persona interessata. Né, sotto il medesimo profilo, l'art. 6.1 condiziona l'emissione di un ordine alla preventiva verifica circa l'integrità dei dati: l'integrità delle prove, infatti, può essere valutata solo dopo, nel momento in cui le autorità competenti dispongono effettivamente delle prove richieste, non già al momento dell'emissione dell'ordine. Infine, sotto il profilo della legalità, l'art. 6.1 non richiede che l'emissione dell'ordine per la prova già acquisita sia sottoposto alle stesse condizioni applicabili per la raccolta iniziale di quelle prove – neppure in una situazione come quella in causa, in cui i dati sono stati raccolti nel territorio dello Stato di emissione e nell'interesse di quest'ultimo –.

Alla luce di questo preciso quadro normativo, allora, nelle dinamiche dell'ordine europeo – sempre a dire della Corte – sono irrilevanti le ragioni e il luogo della raccolta iniziale delle prove da parte dello Stato

[14] Cfr. Cass., sez. un., sent. 29 febbraio 2024, Gjuzi, cit., e Cass., sez. un., sent. 29 febbraio 2024, Giorgi e a., cit., là dove viene individuata la disciplina domestica rilevante ai sensi dell'art. 6 della Direttiva 2014/41/UE: il trasferimento all'autorità giudiziaria italiana del contenuto di comunicazioni effettuate attraverso criptofonini e già acquisite e decrittate dall'autorità giudiziaria estera in altro procedimento penale rientra nella disciplina relativa alla circolazione delle prove tra procedimenti penali, quale desumibile dagli artt. 238 e 270 c.p.p. e 78 disp. att. c.p.p.; mentre l'acquisizione dei risultati di intercettazioni disposte da un'autorità giudiziaria estera in altro procedimento penale ed effettuate su una piattaforma informatica criptata e su criptofonini è assoggettata alla disciplina di cui all'art. 270 c.p.p.

di esecuzione[15]. È, infatti, il principio del mutuo riconoscimento – pietra miliare della cooperazione giudiziaria in materia penale, implicante la fiducia reciproca e il rispetto dei diritti fondamentali – che non autorizza l'autorità di emissione a controllare la regolarità del distinto procedimento con il quale l'autorità di esecuzione abbia raccolto le prove di cui si chiede la trasmissione. D'altra parte, l'art. 14 della direttiva 2014/41 assicura un controllo giurisdizionale *ex post* a garanzia dei diritti fondamentali delle persone interessate. Per un verso, infatti, gli Stati membri assicurano che mezzi di impugnazione equivalenti a quelli disponibili in un caso interno analogo siano applicabili agli atti di indagine richiesti mediante ordine europeo[16] (art. 14.1): spetta, perciò, all'organo giurisdizionale del ricorso controllare il rispetto delle condizioni di emissione di un ordine. Per altro verso, nel procedimento penale avviato nello Stato di emissione, nel valutare le prove acquisite *ultra fines*, devono essere rispettati i diritti della difesa e deve essere garantito un giusto processo (art. 14.7): entro questi limiti, quindi, il procedimento acquisitivo estero viene bensì sottoposto a una *inquiry*.

Eppure, questa lettura, per quanto aderente al testo legislativo, sembra indebolire la doppia clausola di cui all'art. 6.1. Se il fine è prevenire tanto l'abuso della misura di assistenza giudiziaria quanto l'elusione della normativa dello Stato del processo, il fatto che la raccolta iniziale delle prove sia avvenuta con un'intercettazione di massa, su telefonini criptati, mediante basi tecniche inaccessibili e per di più nello Stato di emissione non può che essere rilevante, pur nel silenzio della direttiva.

[15] A tal proposito, la Corte tiene a precisare – seppure incidentalmente – che «nel caso di specie, non risulta che detta raccolta e la trasmissione, mediante un ordine europeo di indagine, delle prove così raccolte abbiano avuto come obiettivo o come effetto [l'elusione delle norme e delle garanzie previste dal diritto dello Stato di emissione], circostanza che spetta al giudice del rinvio verificare» (§ 97).

[16] Anzi, secondo CGUE, sez. I, sent. 11 novembre 2021, causa C-852/19, Gavanozov, il diritto a un ricorso effettivo ai sensi dell'art. 47 della Carta dei diritti fondamentali impone agli Stati di adottare adeguati mezzi di impugnazione nei confronti degli ordini europei suscettibili di incidere sui diritti fondamentali, anche qualora tali mezzi non siano contemplati in un caso interno analogo. Sull'argomento v. *amplius* E. LORENZETTO, *Il diritto a un ricorso effettivo nello Stato di emissione dell'ordine europeo di indagine e le sue rifrazioni nell'ordinamento interno*, in *Cass. pen.*, 2022, p. 838 ss.

Sarebbe stato forse opportuno stabilire una volta per tutte che a vagliare l'impatto di simili prove sui diritti fondamentali sia sempre un organo giurisdizionale proprio dello Stato di emissione sin dal momento dell'adozione della misura di assistenza giudiziaria, almeno quando non sia stato condotto un controllo giurisdizionale 'a monte' dall'autorità di esecuzione nella fase di raccolta iniziale delle prove[17] – così come indirettamente suggerito dall'Avvocato Generale nelle sue conclusioni[18] –.

In fondo, nel diverso contesto in cui opera la Procura europea, la Corte non ha avuto esitazioni a introdurre – senza alcun appiglio nel Regolamento EPPO 2017/1939 – la garanzia del controllo giurisdizionale preventivo a fronte di atti di indagine particolarmente invasivi delle libertà fondamentali[19]. E lo stesso ha già fatto la Corte quando ha imposto l'autorizzazione giurisdizionale per l'accesso ai tabulati telefonici, nella consapevolezza dell'incidenza di una simile attività sulla riservatezza[20].

Proprio sulla scia di queste decisioni particolarmente sensibili alla garanzia della giurisdizione, e pur nella consapevolezza del diverso ambito in cui ci si muove, la Corte avrebbe forse potuto calibrare me-

[17] Non è questo il caso nella vicenda in esame: la raccolta iniziale di prove da parte delle autorità francesi, infatti, era stata autorizzata da un Tribunale.

[18] Cfr. Conclusioni dell'Avvocato Generale Tamara Ćapeta, presentate il 26 ottobre 2023, Causa C-670/22 *Staatsanwaltschaft Berlin c. M.N.*: «74. Quando l'atto di indagine nello Stato di esecuzione è stato autorizzato da un giudice, non è necessario che l'OEI diretto al trasferimento di tali prove sia emesso da un giudice, anche nel caso in cui, ai sensi del diritto dello Stato di emissione, la raccolta delle prove alla base dell'OEI avrebbe dovuto essere disposta da un giudice». Sulla posizione dell'Avvocato Generale, v. *amplius* T. WAHL, *AG: EncroChat Data Can, in Principle, Be Used in Criminal Proceedings*, in *Eucrim*, 8 febbraio 2024 (ultimo accesso il 28 febbraio 2025).

[19] CGUE, grande sez., sent. 21 dicembre 2023, causa C-281/22, G.K. e a., su cui v.: L. PRESSACCO, *I controlli sulle indagini transfrontaliere della Procura europea tra mutuo riconoscimento e armonizzazione indotta*, in *Cass. pen.*, 2024, p. 2400 ss.; e V. SIRELLO, *Il controllo giurisdizionale preventivo nelle indagini transfrontaliere dell'*European Public Prosecutor's Office, in *disCRIMEN* (rivista web), 7 ottobre 2024 (ultimo accesso il 28 febbraio 2025).

[20] CGUE, grande sezione, sent. 2 marzo 2021, causa C-746/18, H.K., su cui v. A. MALACARNE, *"Gravità" dell'ingerenza e "terzietà" dell'organo titolare del potere autorizzatorio: vecchi e nuovi principi in materia di* data retention, in *Riv. it. dir. proc. pen.*, 2021, p. 1164 ss.

glio la sua decisione nel caso "Encrochat", allineando a un unico *standard* – il più elevato – la possibilità di acquisire le prove digitali in possesso di un altro Stato membro.

2.1.2. La questione dell'utilizzabilità della prova

L'altra questione pregiudiziale posta dal giudice del rinvio rilevante ai fini del nostro discorso riguarda il principio di effettività e le conseguenze giuridiche di un'acquisizione di prove in violazione del diritto dell'Unione. Il Tribunale di Berlino chiede, in sostanza, se, riscontrata l'illegittimità degli ordini europei emessi dalla procura generale di Francoforte, sia tenuto a escludere i mezzi di prova pur ottenuti dalle autorità francesi.

La Corte inizialmente ribadisce che spetta unicamente al diritto nazionale disciplinare l'ammissibilità e la valutazione di prove ottenute con modalità contrarie al diritto dell'Unione, così come spetta all'ordinamento di ciascuno Stato membro assicurare i ricorsi a tutela dei diritti spettanti ai singoli in forza del diritto dell'Unione, purché nel rispetto dei principi di equivalenza e di effettività. D'altra parte, l'art. 14.7 della direttiva 2014/41 – come già evidenziato – impone espressamente agli Stati membri di assicurare che nel processo nello Stato di emissione siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove acquisite tramite l'ordine europeo. È, dunque, proprio l'art. 14.7 quale strumento di *inquiry ex post* a imporre al giudice penale nazionale di espungere informazioni ed elementi di prova sui quali l'imputato non sia in grado di svolgere efficacemente le proprie osservazioni e che siano idonei a influire in modo preponderante sulla valutazione dei fatti – un principio poi sostanzialmente ribadito dai giudici italiani sempre nella vicenda Sky-ECC[21] –.

[21] Cfr. Cass., sez. un., sent. 29 febbraio 2024, Gjuzi, cit., e Cass., sez. un., sent. 29 febbraio 2024, Giorgi e a., cit.: l'autorità giurisdizionale dello Stato di emissione dell'ordine europeo di indagine deve verificare il rispetto dei diritti fondamentali, comprensivi del diritto di difesa e della garanzia di un equo processo. Su questo punto, le Sezioni Unite hanno ulteriormente specificato che, a fronte di una presunzione relativa di conformità ai diritti fondamentali dell'attività svolta dall'autorità giudiziaria estera, è onere della difesa allegare e provare i fatti dai quali dipende la violazione denunciata.

La Corte ritorna quindi parzialmente su quanto già affermato di sfuggita: se la verifica dell'integrità dei dati ottenuti può essere effettuata solo dopo che le autorità competenti dispongano effettivamente di quanto richiesto, è al momento dell'ammissione di questi dati ovvero del contraddittorio su di essi – o al più tardi al momento della loro valutazione – che l'eventuale opacità dell'iniziale attività acquisitiva assume il dovuto rilievo, certamente nel caso in cui si tratti di elementi probatori decisivi[22].

Viene così affermato un principio di trasparenza, che, nel caso di specie, si giustifica a fronte del segreto militare opposto dalle autorità francesi, ma che ben potrà esercitare il suo impatto nelle ipotesi di prove acquisite mediante intelligenza artificiale le cui basi tecniche risultino imperscrutabili al di là di ragioni strettamente politiche (per esempio per ragioni commerciali o per un segreto industriale). D'altra parte, che la trasparenza del procedimento di acquisizione delle prove digitali[23] sia un diritto della difesa promanante dalla parità delle armi, a sua volta espressione del diritto a un equo processo, lo sottolinea da tempo la più attenta dottrina[24], oltre che la giurisprudenza di Strasburgo[25].

[22] È forte l'assonanza con il principio elaborato in una proposta di direttiva sull'ammissibilità reciproca delle prove e delle prove elettroniche nei procedimenti penali, avanzata da un gruppo di studiosi nell'ambito di un progetto condotto dallo *European Law Institute*, consultabile all'indirizzo web: *https://www.europeanlawinstitute.eu/news-events/news-contd/news/eli-publishes-a-legislative-proposal-on-mutual-admissibility-of-evidence-and-electronic-evidence-in/* (ultimo accesso il 28 febbraio 2025) su cui sia consentito rinviare a R. BELFIORE, *Quali prospettive per l'ammissibilità reciproca delle prove tra gli Stati membri dell'Unione europea?*, in *Cass. pen.*, 2023, p. 3870 ss.

[23] Si pensi all'accesso agli originali delle comunicazioni e all'algoritmo impiegato per la loro decriptazione, nel caso di telecomunicazioni cifrate.

[24] Cfr., *inter alia*: A. GAITO, *Comunicazioni criptate ed esigenze difensive (da Blackberry a Sky-ECC)*, in *Archivio penale*, 2024, 1, p. 8 ss.; E. LORENZETTO, *L'acquisizione all'estero di comunicazioni digitali criptate nella fucina dell'ordine europeo di indagine penale*, in *Cass. pen.*, 2024, p. 185 s.; e J.J. OERLEMANS, D. VAN TOOR, *op. cit.*, p. 314 s.

[25] V., da ultimo, C. eur. dir. uomo, grande camera, sent. 26 settembre 2023, *Yuksel Yalçinjaya c. Turchia*. Sulla giurisprudenza europea in argomento, si rinvia a M. PISATI, *'Full collection of data' e diritto di difesa*, in *Riv. it. dir. proc. pen.*, 2019, p. 2239 ss.

2.2. La Procura europea

Se questo è quanto accade nell'area dell'assistenza giudiziaria propriamente intesa, resta ancora da vedere cosa ne sarà della prova digitale nel quadro giuridico in cui opera il pubblico ministero europeo. Il Regolamento EPPO 2017/1939[26] non presenta specifiche norme concernenti l'acquisizione di dati e informazioni digitali nel caso di indagini transfrontaliere. L'art. 37 si limita a disporre che le prove presentate dai procuratori dell'EPPO o dall'imputato non siano escluse per il solo motivo che sono state raccolte in un altro Stato membro o conformemente al diritto di un altro Stato membro. L'art. 30, dal canto suo, prevede che, qualora si indaghi per reati piuttosto gravi e indipendentemente dalla transnazionalità del caso, i procuratori europei delegati (PED) siano legittimati a disporre o a chiedere tutta una serie di misure investigative, tra cui: la perquisizione di sistemi informatici; la produzione di dati informatici, cifrati o decifrati; l'intercettazione di comunicazioni elettroniche; il tracciamento di un oggetto mediante mezzi tecnici.

Orbene, in assenza di più dettagliate norme regolamentari, non pare possibile prescindere dalla menzionata sentenza in cui la Corte ha ritenuto che la misura investigativa assegnata dal PED di uno Stato al PED di un altro debba essere sottoposta a un previo controllo giurisdizionale effettuato nello Stato del PED incaricato del caso in situazioni di grave ingerenza nei diritti fondamentali[27]. Si tratta di una decisione niente affatto scontata, in assenza di un appiglio nel Regolamento EPPO; una decisone che non potrà che riverberarsi anche sull'acquisizione transnazionale di prove digitali. Si pensi, in particolare, al 'nostro' sequestro probatorio, che, quand'anche effettuato su dati informatici, è di esclusiva prerogativa del pubblico ministero, e dunque del PED italiano nel caso di indagini su reati che ledono gli interessi finanziari dell'Unione: una misura che non dovrebbe più poter essere condivisa all'interno dell'ufficio della procura europea senza una previa autorizzazione del giudice per le indagini preliminari.

[26] Regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea.

[27] CGUE, grande sezione, sent. 30 aprile 2024, Causa C-670/22, M.N., cit.

Non a caso, è al momento in discussione una proposta di legge per la modifica al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici, *smartphone* e memorie digitali, con cui – tra le altre cose – si intende introdurre una riserva di giurisdizione, sia nel caso di sequestro di dispositivi che nel caso di sequestro di dati comunicativi[28].

2.3. L'ordine europeo di produzione e conservazione di prove elettroniche

Infine, merita qualche breve cenno l'ultimo possibile scenario di cooperazione giudiziaria a livello eurounitario riguardante specificatamente la circolazione di dati digitali, schiuso dal recente Regolamento 2023/1543 sugli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali, adottato unitamente alla direttiva 2023/1544 sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali[29].

Si tratta di uno scenario ancora tutto da vedere, non soltanto perché il Regolamento si applicherà solo a partire dal 18 agosto 2026 (la direttiva, invece, andrà recepita entro il 18 febbraio dello stesso anno), ma soprattutto perché questo scenario apre a forme di assistenza inedite, in parte già delineate dal menzionato II Protocollo addizionale alla Convenzione di Budapest del 2022, tuttavia non ancora in vigore. Alla cooperazione giudiziaria fra Stati sovrani si sostituisce una cooperazione diretta tra Stati e società private, al fine di non disperdere ovvero acqui-

[28] Sul punto v.: S. DE FLAMMINEIS, *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, in *Sistema penale* (rivista web), 8 marzo 2024 (ultimo accesso il 28 febbraio 2025); O. MURRO, *Sequestro dei dispositivi informatici: verso l'art. 254 ter c.p.p.? Brevi note a margine del d.d.l. A.S. n. 806*, in *Penale Diritto e Procedura* (rivista web), 12 marzo 2024 (ultimo accesso il 28 febbraio 2025); ed EAD., *Lo* smartphone *come fonte di prova*, cit., p. 261 ss.

[29] V. *amplius* T. WAHL, *E-evidence Regulation and Directive Published*, in *Eucrim*, 9 novembre 2023 (ultimo accesso il 28 febbraio 2025).

sire dati probatori più velocemente e quindi più efficacemente[30]. Le società private coinvolte non sono altro che gli *Internet Service Provider*, ossia i prestatori di servizi di comunicazione elettronica (*email*), di nomi di dominio internet e di numerazione IP, ovvero di servizi della società dell'informazione (come i *social network* o i prestatori di servizi di *hosting*), qualora offrano i loro servizi nell'Unione europea e perciò abbiano inderogabilmente designato uno stabilimento o nominato un rappresentate legale ai fini proprio della ricezione, dell'ottemperanza e dell'esecuzione di decisioni e ordini emessi per acquisire prove elettroniche nei procedimenti penali[31].

Le ragioni di una simile opzione si spiegano con le difficoltà che porrebbe l'individuazione dello Stato cui rivolgere un'eventuale domanda di assistenza per la prova digitale[32]. Non sempre, infatti, è agevole ancorare il dato a un certo territorio. Lo si è detto: sono molteplici o solo virtuali i "luoghi" che vengono in rilievo quando si tratta di prove digitali. Ecco allora che si è deciso di promuovere un metodo alternativo alle classiche forme di cooperazione giudiziaria: la richiesta diretta (o, più correttamente, l'ingiunzione di produzione) di dati probatori di interesse da parte dell'autorità giudiziaria di uno Stato ai rappresentanti legali dei *service provider* in un altro Stato, in aperta antitesi alla c.d. *voluntary disclosure*, altrimenti l'unica modalità per l'autorità di ottenere la collaborazione dei prestatori di servizi[33]. E infatti, quando, pur ricorrendone le condizioni e in assenza di giustificati motivi, gli ordini non vengono eseguiti entro i termini previsti, i *provider* possono

[30] Cfr. M. DANIELE, *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Revista Brasileira de Direito Processual Penal*, 2019, p. 1277 ss.

[31] Cfr. gli artt. 1 e 3 della direttiva (UE) 2023/1544.

[32] Si chiede M. DANIELE, *op. cit.*, p. 1281: «Come identificare […] lo Stato di esecuzione? Dovrebbe essere lo Stato in cui opera o ha la sede legale il *service provider* che ha accesso alle prove? Oppure dovrebbe essere lo Stato in cui si trova il *server* dove le prove sono reperibili, magari diverso dallo Stato del *provider*? E in quest'ultimo caso, come effettuare la scelta qualora, come spesso accade per ragioni economiche od organizzative, le prove vengano fatte costantemente circolare fra *server* situati in Stati diversi (c.d. *load balancing*)?». In termini analoghi, v. già F. SIRACUSANO, *op. cit.*, p. 180.

[33] Così M. DANIELE, *op. cit.*, p. 1282.

essere sottoposti a sanzioni pecuniarie da parte degli Stati in cui essi hanno la loro sede legale[34]. Anzi, ancor prima, i *provider* possono essere sottoposti alla procedura di 'esecuzione coatta' con il coinvolgimento dello Stato di esecuzione, individuato nello Stato in cui ha sede o è rappresentato il prestatore di servizi[35]. Quest'ultimo Stato – si segnala – può essere coinvolto anche quando gli sia dovuta una notifica, tuttavia esclusa se «un ordine europeo di produzione sia emesso per ottenere prove elettroniche in procedimenti penali con legami forti e sostanziali con lo Stato di emissione»[36].

L'ordine di produzione (per la trasmissione di dati) e l'ordine di conservazione (per la custodia di dati) possono avere ad oggetto tre tipi di dati: quelli relativi agli 'abbonati' (sostanzialmente i loro dati anagrafici, il tipo di servizio utilizzato e la sua durata, nonché l'indirizzo IP solo ai fini identificativi dell'utente); quelli relativi al 'traffico' (riguardanti la fornitura del servizio, ossia la fonte e il destinatario di un messaggio o altro tipo di interazione, l'ubicazione del dispositivo, etc.); e quelli relativi al 'contenuto' (dati in formato digitale come testo, voce, video, immagini o suono).

A seconda dell'oggetto dell'ordine di produzione e dell'intensità del suo impatto sui diritti fondamentali varia il livello di garanzie offerte. Mentre nel caso di produzione di dati relativi all'abbonato è previsto un ricorso *ex post* davanti a un organo giurisdizionale (è garantito, cioè, un mezzo di impugnazione nello Stato di emissione), nel caso di produzione di dati relativi al traffico ovvero al contenuto è altresì assicurato un vaglio giurisdizionale *ex ante* (è garantita, cioè, la previa autorizzazione o convalida di un giudice, sempre nello Stato di emissione). In linea con questa ideale gradualità dell'invasività dello strumento, gli ordini di conservazione, invece, possono essere emessi da un pubblico ministero senza alcun controllo giurisdizionale, nemmeno successivo.

[34] Cfr. gli artt. 15 e 16 del Regolamento (UE) 2023/1543.

[35] Cfr. l'art. 16 del Regolamento (UE) 2023/1543.

[36] Così testualmente il considerando n. 51 del Regolamento (UE) 2023/1543. Invero, ai sensi dell'art. 8, la notifica non è dovuta se, al momento dell'emissione dell'ordine, l'autorità di emissione ha fondati motivi di ritenere che: a) il reato sia stato commesso, sia in atto o sia suscettibile di essere commesso nello Stato di emissione; e b) la persona i cui dati sono richiesti risieda nello Stato di emissione.

Ebbene, pure là dove un controllo giurisdizionale è opportunamente previsto, questa nuova modalità di acquisizione dei dati digitali sembra determinare l'assoluta egemonia dello Stato di emissione, in un rapporto – come si diceva per lo più bilaterale, Stato di emissione-*Internet service provider* – sbilanciato, in cui il rispetto dei diritti fondamentali non è condiviso tra Stati sovrani ma piuttosto conteso tra soggetti tra loro eterogenei, portatori di interessi tutti meritevoli di tutela. Da un lato l'autorità giudiziaria, concentrata sull'attività di contrasto al crimine, e dall'altro il prestatore di servizi, animato dalla libertà d'impresa e dall'esigenza di preservare i rapporti con i propri clienti. In mezzo, il povero titolare dei dati digitali, in balia di questa contesa. Peraltro, sebbene al titolare dei dati sia riconosciuto il diritto all'informazione circa la produzione dei dati e il diritto a un ricorso effettivo contro l'ordine di produzione, questi diritti devono essere pur sempre assicurati dal solo Stato di emissione[37], confermando quell'egemonia di cui si diceva, di norma estranea ai rapporti di cooperazione giudiziaria in senso stretto, in cui la tutela giurisdizionale è appunto condivisa tra Stati sovrani.

Certo, ci sono anche vantaggi in questo nuovo paradigma di assistenza: la riduzione del carico giudiziario nei rapporti interstatuali; la rapidità e la maggiore efficienza dell'approvigionamento probatorio a favore della ragionevole durata del processo[38]; e chissà, forse una maggiore trasparenza a servizio della certezza del diritto[39]. Vedremo cosa accadrà. Sarà doveroso vigilare.

[37] Particolarmente critico al riguardo P. TOPALNAKOS, *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, in *Eucrim*, 2023, 2, p. 202.

[38] In tal senso, v. O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, in *Leg. pen.* (rivista web), 30 marzo 2021, p. 41 (ultimo accesso il 28 febbraio 2025).

[39] In questi termini N.A. SMUHA, *Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency*, in *European Criminal Law Review*, 2018, p. 101.

INTERCETTAZIONI E TUTELA DEI TERZI ESTRANEI AL PROCEDIMENTO

Marianna Biral

SOMMARIO: *1. Il caso Contrada n. 4. 2. Fisionomia del rimedio: quale controllo? Quali terzi? 3. Possibili strade per un allineamento del diritto interno agli orizzonti europei: interpretazione convenzionalmente orientata dell'art. 269, co. 2 c.p.p…. 4. …o creazione di un rimedio* ad hoc*?*

1. Il caso Contrada n. 4

> Il diritto italiano non prevede garanzie adeguate ed effettive che proteggano dal rischio di abuso le persone interessate da una misura di intercettazione le quali, non essendo sospettate di essere implicate in un reato né imputate dello stesso, rimangono estranee al procedimento. In particolare, non è previsto che tali persone abbiano la facoltà di rivolgersi a un'autorità giudiziaria per ottenere un controllo efficace della legalità e della necessità della misura e per ottenere, se del caso, una riparazione appropriata[1].

È questa la diagnosi alla base dell'accoglimento del ricorso Contrada n. 4, nella parte dedicata alle intercettazioni[2]. La sua portata ampia e generalizzante, condensata in quel riferimento insistito a un deficit strutturale della disciplina interna (*il diritto italiano non prevede garan-*

[1] Corte eur. dir. uomo, sez. I, sent. 23 maggio 2024, Contrada c. Italia (n. 4), § 92. Traduzione a cura del Ministero della Giustizia.

[2] Il ricorso porta all'attenzione della Corte anche altre questioni (legate alla perquisizione domiciliare subita da Contrada), che non saranno esaminate in questa sede. Per un approfondimento, si rinvia a L. GIORDANO, *Considerazioni sulla sentenza della Cedu Contrada c. Italia n. 4: per un'interpretazione convenzionalmente orientata delle norme del codice di rito*, in *Sistema penale* (rivista web), 26 giugno 2024 (ultimo accesso il 28 febbraio 2025); E. SCORZA, *Diritto al rispetto della vita privata, procedimento penale e mezzi di ricerca della prova: la Corte edu si pronuncia sulla tutela dei terzi*, in *Cass. pen.*, 2024, 9, p. 2840 ss.

zie adeguate), schiude prospettive d'analisi altrettanto ampie e sfidanti. Lo scenario non è quello – al fondo rassicurante – d'un sistema che funziona ma che nel caso di specie si è inceppato, bensì d'un sistema fallato, e pertanto da ripensare. Non solo: a essere finito nell'occhio del ciclone è un mezzo di ricerca della prova che non riesce a trovare pace, costantemente al centro di polemiche e discussioni, riforme e controriforme[3].

Riavvolgiamo dunque il filo, e ricostruiamo i passaggi che hanno portato la Corte europea dei diritti dell'uomo a formulare quella netta valutazione. A partire dalle circostanze di fatto alla base del ricorso. Il 29 giugno 2018 il domicilio e altri due immobili nella disponibilità di Bruno Contrada sono sottoposti a perquisizione nell'ambito di un'indagine mirata a far luce sull'omicidio di un agente di polizia; indagine in cui – è un dato importante – il ricorrente non figura (e non figurerà mai) fra i sospettati né è coinvolto ad altro titolo. Leggendo il mandato, Contrada apprende d'essere stato intercettato, ma né in quel momento né nelle settimane e mesi successivi riceve alcuna notifica delle decisioni giudiziarie di autorizzazione e proroga della sorveglianza occulta operata sulle sue utenze telefoniche (il sistema, del resto, non lo prevede). L'11 dicembre di quello stesso anno decide di rivolgersi alla Corte per denunciare un'ingerenza ingiustificata nella propria vita privata e familiare.

Il ricorso è giudicato ricevibile: è positivamente accertata sia la qualità di vittima dell'interessato sia il previo esaurimento delle vie di ricorso interne.

Sotto il primo profilo, il giudice europeo ritiene pacifico che, essendo stato bersaglio d'un provvedimento d'intercettazione, Contrada abbia titolo per lamentare una violazione dei diritti sanciti dall'art. 8 Cedu[4].

[3] A fotografare quel che si muove oggi sul terreno delle intercettazioni – i moti riformatori più recenti, le questioni scottanti che affollano i repertori di giurisprudenza e le riviste scientifiche – ci ha pensato S. RENZETTI, *"Qualcosa è cambiato": vecchio e nuovo in tema di intercettazioni*, in *Jus*, 2024, f. 1, p. 141 ss.

[4] In ordine ai presupposti per invocare la qualità di vittima ai sensi dell'art. 34 Cedu, v., fra le tante, Corte eur. dir. uomo, grande camera, sent. 17 luglio 2014, Centro di risorse giuridiche in nome di Valentin Câmpeanu c. Romania, § 96.

Quanto alla regola che impone di avvalersi dei rimedi offerti dall'ordinamento nazionale prima di adire la Corte di Strasburgo, la conclusione è che il governo italiano non abbia assolto all'onere di dimostrare che il ricorrente, rimasto inerte, avrebbe potuto coltivare un ricorso adeguato per vedere riconosciute le proprie istanze e prevenire la violazione dedotta[5]. In particolare, delle tre vie indicate, due sono giudicate impraticabili, una ineffettiva.

Partiamo da quest'ultima. Il resistente chiama in causa il meccanismo disciplinato dall'art. 269, co. 2 c.p.p., il quale abilita gli «interessati» a chiedere la distruzione delle intercettazioni «quando la documentazione non è necessaria per il procedimento». La Corte, tuttavia, non condivide: la disposizione – è vero – offre alle persone non direttamente coinvolte nel procedimento la possibilità di adire il giudice che ha disposto o convalidato la misura a tutela della propria riservatezza; il problema, tuttavia, risiede nel contenuto del controllo per questa via sollecitato, che non comprendendo una valutazione circa la legittimità del provvedimento "a monte" della captazione, non rappresenta, secondo le categorie della Corte, un rimedio effettivo[6].

Le ulteriori opzioni prospettate dal governo italiano sono liquidate in poche righe. Da una parte, il dovere del giudice di ordinare la distruzione delle intercettazioni illegittimamente disposte o eseguite (art. 271 c.p.p.) non può essere invocato da chi, come Contrada, non è parte nel procedimento (§ 71); dall'altra, la possibilità, in linea teorica sempre disponibile, di rivolgersi alla Corte di Cassazione allo scopo di far riconoscere il carattere abnorme d'una decisione giudiziaria non costituiva una via di ricorso percorribile nel caso di specie: il governo «non ha dimostrato che il mandato in contestazione potesse essere considerato

[5] Quando è sollevata un'eccezione di mancato esaurimento delle vie di ricorso interne, l'onere della prova è ripartito in questo modo: spetta al governo che contesta il mancato rispetto della regola convincere la Corte dell'esistenza, all'epoca dei fatti, di rimedi adeguati e disponibili; una volta che ciò è dimostrato, la palla passa al ricorrente sul quale grava il compito di provare che il ricorso citato dal governo è stato di fatto esperito, ma che non era effettivo. V. Corte eur. dir. uomo, grande camera, sent. 10 settembre 2010, McFarlane c. Irlanda, § 107.

[6] «Da un'analisi della giurisprudenza pertinente della Corte risulta che, per essere effettivo ai fini dell'esaurimento delle vie di ricorso interne, un ricorso deve anzitutto permettere un controllo della legalità e della necessità della misura» (§ 51).

un atto "abusivo" […] e, in quanto tale, impugnabile direttamente per cassazione» (§ 72).

Sciolto il nodo dell'ammissibilità, la Corte di Strasburgo ragiona intorno alla fondatezza della questione.

Il nocciolo della censura fa perno sulla ritenuta mancanza, nella disciplina italiana sulle intercettazioni, di una base legale adeguata, capace di offrire sufficienti garanzie contro l'arbitrarietà. In particolare, sono due le criticità segnalate dal ricorrente: l'assenza, nel corpo dell'art. 267 c.p.p., d'un riferimento specifico alle categorie di persone assoggettabili a sorveglianza occulta; l'omessa previsione d'un controllo giudiziario *ex post* sulla misura attivabile dal terzo estraneo al procedimento.

Il primo motivo è respinto, il secondo fa breccia. Da una parte, la Corte esclude problemi di chiarezza e prevedibilità della normativa poiché, se pure la legge non reca un'indicazione specifica delle categorie di persone intercettabili, esiste una giurisprudenza consolidata – nel cui solco si è posto il giudice del caso di specie – che esige motivazioni stringenti dei provvedimenti autorizzativi; motivazioni in cui vanno indicati, fra l'altro, i collegamenti esistenti fra l'indagine e il soggetto interessato dalla misura. Ed è un tassello, questo, che s'inserisce in un mosaico più ampio – una disciplina di presupposti e regole di esecuzione del mezzo di ricerca della prova articolata e nel complesso rigorosa – che la stessa Corte ha in più occasioni promosso[7]. D'altra parte, però, rileva un deficit di tutela rispetto alla specifica posizione del terzo. Non solo non è prevista alcuna notifica successiva della misura cosicché questa persona, salvo indiscrezioni o caso fortuito, potrebbe non venire mai a sapere d'essere stata sottoposta a sorveglianza segreta; ma se anche ne venisse in qualche modo a conoscenza, non disporrebbe di alcun ricorso utile a sollecitare un controllo giudiziario sull'ingerenza subita[8]. Di qui, si arriva alla diagnosi da cui siamo partiti; la Corte ritiene che il diritto italiano «non soddisfi il requisito relativo alla qualità della legge e non sia in grado di limitare l'ingerenza a quanto necessario in una

[7] Corte eur. dir. uomo, sent. 23 maggio 2024, Contrada c. Italia (n. 4), § 90.

[8] Sono richiamate, a questo proposito, le osservazioni svolte (in punto di ammissibilità del ricorso) per respingere l'eccezione di mancato esaurimento delle vie di ricorso interne.

società democratica»[9] e che questo abbia determinato, nel caso di specie, una violazione dell'art. 8 Cedu.

2. Fisionomia del rimedio: quale controllo? Quali terzi?

La Corte europea esige dall'ordinamento italiano una revisione degli spazi di tutela accordati al terzo estraneo al procedimento in rapporto alle intercettazioni: è questa l'eco che si spande dalla sentenza Contrada n. 4. Per comprendere come costruire questi spazi di tutela occorre approfondire alcuni aspetti.

Per prima cosa, il tipo di controllo che quel rimedio effettivo dovrebbe favorire. Sul punto, la linea di Strasburgo è piuttosto chiara: occorre che anche chi non è indagato o imputato possa contestare la necessità e proporzionalità della misura disposta nei suoi confronti e, se del caso, ottenere un'equa riparazione[10]. L'accesso a un organo imparziale, che abbia titolo per verificare la *lawfulness* (nella sostanza, presupposti e modalità esecutive) del provvedimento autorizzativo del mezzo di ricerca della prova, rappresenta infatti una garanzia fondamentale per mettere al riparo l'individuo – anche chi non è coinvolto nel processo – dagli abusi dell'autorità[11]. Il tipo di controllo tratteggiato chiama in causa il giudice penale: è a lui che fisiologicamente spetta la supervisione delle misure di sorveglianza disposte a fini di accertamento dei reati. Di qui, la considerazione per cui la legge processuale pena-

[9] Corte eur. dir. uomo, sent. 23 maggio 2024, Contrada c. Italia (n. 4), § 96.

[10] Il carattere appropriato e sufficiente della riparazione che spetta a chi vede limitati i diritti riconosciuti dall'art. 8 Cedu dipende dalle circostanze del caso e dalla posizione del ricorrente (se parte del processo penale o meno). Può consistere nell'esclusione dal fascicolo processuale (Corte eur. dir. uomo, sent. 8 febbraio 2028, Ben Faiza c. Francia, §§ 47 e 73), nella distruzione (Corte eur. dir. uomo, sent. 23 giugno 2022, Haščák c. Slovacchia) delle conversazioni "incriminate" o anche in un risarcimento pecuniario (Corte. eur. dir. uomo, dec. 9 aprile 2024, Gernelle e S.A. Société d'Expoliation de l'Hebdomadaire *Le Point* c. Francia, §§ 52-54). Delle varie opzioni in elenco, è evidente che la prima non viene in gioco quando l'interessato è un soggetto non coinvolto nel processo penale.

[11] Principio ribadito, più di recente, in Corte eur. dir. uomo, sent. 28 novembre 2024, Klaudia Csikós c. Ungheria, in particolare §§ 50 e 59-71.

le rappresenta probabilmente il settore più adeguato entro cui coltivare utilmente la strada per un allineamento con i parametri della Convenzione europea[12].

Bisogna mettere a fuoco, poi, la latitudine del rimedio. La pronuncia in commento – l'abbiamo detto – riguarda un soggetto *direttamente* intercettato, le cui utenze telefoniche, cioè, hanno costituito proprio il bersaglio preso di mira dal provvedimento che ha autorizzato l'attività di captazione[13]. Ma che dire degli *altri terzi*, di quelli le cui conversazioni finiscono nella rete gettata dagli inquirenti perché entrano in contatto con chi è sottoposto a controllo o di quelli che vengono menzionati nelle conversazioni registrate con effetti pregiudizievoli sul piano della reputazione? Dovrebbero essere legittimati pure loro a sollecitare il vaglio del giudice?

Rispondere a queste domande non è semplice né banale, e i segnali che arrivano dalla Corte sul punto non sono univoci.

Non c'è dubbio che anche questi soggetti subiscono una violazione della vita privata e familiare, e, in quanto "vittime" ai sensi dell'art. 8 Cedu[14], dovrebbero poter contare sull'intero fascio di garanzie che da quella disposizione si dipana, compresa per l'appunto la possibilità di attivare una verifica *ex post* sulla legittimità dell'intercettazione. Si colloca in questo solco la sentenza Pruteanu c. Romania del 2015[15], che ha accolto il ricorso di un individuo *randomly affected* da un'attività di sorveglianza occulta disposta nell'ambito di un procedimento per truffa. Il caso è particolare: il ricorrente è il difensore di uno degli indagati, e della cognata di questi, estranea ai fatti di causa ma sottoposta a inter-

[12] È del resto in questa direzione che si sono mossi i primi commentatori della pronuncia. L. GIORDANO, *Considerazioni sulla sentenza della Cedu Contrada c. Italia n. 4*, cit.; E. SCORZA, *Diritto al rispetto della vita privata, procedimento penale e mezzi di ricerca della prova*, cit., p. 2840.

[13] Al titolare dell'utenza va equiparata la posizione dell'utilizzatore effettivo. V. Corte eur. dir. uomo, sent. 12 gennaio 2023, Potoczká e Adamčo c. Slovacchia.

[14] È un'affermazione di principio che risale a Corte eur. dir. uomo, grande camera, sent. 16 febbraio 2000, Amman c. Svizzera (vedi, in particolare, § 45) e si è nel tempo consolidata, diventando un punto fermo nell'esegesi della disposizione. In dottrina, v. S. LORUSSO, *Intercettazioni e Cedu. Un circuito a geometria variabile*, in P. MAGGIO (a cura di), *La nuova disciplina delle intercettazioni*, Torino, 2023, p. 11.

[15] Corte eur. dir. uomo, sent. 3 febbraio 2025, Pruteanu c. Romania.

cettazione per via dei rapporti familiari che la legano ai sospettati (uno – come dicevamo – è il cognato e l'altra la sorella) e del ruolo rivestito nella società cui è contestato l'illecito. Sono proprio le conversazioni che il ricorrente intrattiene con la cliente non indagata a essere oggetto del ricorso alla Corte europea. Egli lamenta un'ingerenza illegittima nella propria vita privata, dovuta fra l'altro alla mancata possibilità di attivare – in proprio e non in rappresentanza di interessi dei suoi assistiti – un controllo sulla legittimità misura. La Corte gli dà ragione e condanna lo Stato rumeno.

Aderisce alla medesima impostazione anche la più recente Plecho c. Slovacchia[16]. Nell'ambito di una vasta indagine per fatti di corruzione legati ad attività dell'agenzia nazionale per le privatizzazioni (*National Property Fund*), sono disposte intercettazioni telefoniche che attingono in via indiretta anche il ricorrente. Lo toccano indirettamente perché questi, pur essendo un alto funzionario dell'ente finito sotto inchiesta, non solo non figura fra gli indagati, ma nemmeno risulta – alla luce del materiale visionato dalla Corte – fra i *target* della sorveglianza; le sue telefonate sono state registrate e acquisite agli atti del procedimento per via dei contatti che egli aveva avuto con alcuni dei soggetti intercettati nel periodo in cui le loro utenze erano sottoposte a controllo. Una volta venuto a conoscenza dell'esistenza di registrazioni che lo riguardano, avvia una serie di iniziative legali volte a contestare il provvedimento autorizzativo della misura e a ottenere la distruzione del materiale raccolto a lui riferibile. Non ha buona fortuna e si rivolge pertanto al giudice europeo, il quale, anche in questo caso, ravvisa una violazione dell'art. 8 Cedu[17].

Sono precedenti che in effetti puntano in una certa direzione, verso una tutela "estesa" dei terzi estranei al procedimento (il rimedio spetta a tutti gli intercettati, a prescindere dal fatto che la misura li abbia attinti in via diretta o indiretta); e tuttavia è bene non sopravvalutarne la cogenza. In entrambi i casi, infatti, il contesto in cui i ricorsi affondano le

[16] Corte eur. dir. uomo, sent. 26 ottobre 2023, Plecho c. Slovacchia.

[17] «The Court concludes that the interference with the applicant's right to respect for his private life and correspondence was not accompanied by adequate and effective guarantees against abuse» (Corte eur. dir. uomo, sent. 26 ottobre 2023, Plecho c. Slovacchia, § 50).

proprie radici è particolare. Nel primo, viene in gioco la tutela del rapporto difensore-cliente che, pur non intenzionalmente violata dagli inquirenti, s'intreccia – rendendola più delicata – alla questione del rispetto della vita privata e familiare. Nel secondo, l'attività investigativa condotta dalle autorità slovacche è coeva, e in qualche modo legata, a una spregiudicata operazione di intercettazione e dossieraggio su larga scala (l'"operazione Gorilla") condotta nei primi anni Duemila dai servizi segreti, la quale aveva già procurato alla Slovacchia alcune condanne da parte dei giudici di Strasburgo, basate fra l'altro sulla diagnosi di vistosi profili d'inadeguatezza della disciplina delle intercettazioni[18]. Il peso che queste condizioni di contesto hanno avuto nel ragionamento sviluppato nel caso Plecho si coglie, in particolare, nel passaggio della pronuncia in cui la Corte mette in relazione l'interesse del ricorrente ad avere accesso e sollecitare un controllo sul *warrant* – riguardante, va da sé, non lui ma altre persone – con lo stato della legge slovacca che aveva portato, in condizioni di tempo e contesto analoghe, all'adozione di provvedimenti autorizzativi contrassegnati da «systemic flaws of an objective character»[19].

C'è anche un altro aspetto da considerare: non sono rare le occasioni in cui il giudice europeo sottolinea la distanza fra le posizioni di chi è direttamente intercettato e chi invece viene toccato dall'attività investigativa solo di riflesso. Lo fa anche nella sentenza Contrada n. 4, al § 88, sebbene senza dedurne – quantomeno non esplicitamente – alcuna ricaduta sul diritto al rimedio in discussione.

Eppure, la differenza fra le due classi di terzi estranei al procedimento sembra rilevare proprio in relazione all'interesse a impugnare il provvedimento genetico della misura di sorveglianza. Non ci sono dubbi, infatti, che anche la *random party* di un'intercettazione subisca una restrizione della libertà e segretezza delle proprie comunicazioni oltreché della privacy, e debba poter agire a tutela dei propri diritti (per esempio, chiedendo la distruzione delle registrazioni che non rilevano a fini processuali), ma è discutibile che abbia un interesse giuridicamente apprezzabile a contestare un provvedimento che *riguarda altri* e ridon-

[18] V. in particolare Corte eur. dir. uomo, sent. 20 luglio 2021, Zoltán Varga c. Slovacchia.

[19] Corte eur. dir. uomo, sent. 26 ottobre 2023, Plecho c. Slovacchia, § 44.

da su di lui o lei solo di riflesso e per ragioni che hanno a che fare, in buona sostanza, con il caso. Ragionevolmente, la chiave per distinguere chi ha titolo per chiedere un controllo sulla legittimità della captazione da chi non ne ha dovrebbe essere la *direzione* dell'attività investigativa[20]: se il soggetto è il *target* della sorveglianza occulta, l'interesse si configura; se il soggetto è toccato incidentalmente – e casualmente – dalla misura, l'interesse non c'è[21].

Esistono, peraltro, anche ragioni pratiche e di opportunità che consigliano di muoversi in questa direzione. Un meccanismo azionabile da una platea di persone potenzialmente vastissima – si pensi a intercettazioni che si protraggono a lungo, magari per l'intero arco temporale delle indagini – si candida a essere non sostenibile: molto difficile costruire spazi di intervento effettivo per tutti senza sovraccaricare il sistema.

Sotto altro profilo, va osservato come la scelta di dar voce al terzo non solo sulla rilevanza/necessità dei risultati delle intercettazioni, ma

[20] In linea rispetto a quanto prevede l'art. 252-*bis* c.p.p. in tema di opposizione alle perquisizioni domiciliari "negative": sono legittimate le persone «nei cui confronti la perquisizione è stata disposta o eseguita» – anche qui, è la direzione dell'attività a tracciare il perimetro della legittimazione attiva. D'altra parte, la tesi non è contraddetta dalla situazione che si configura rispetto al sequestro probatorio, in relazione al quale sono abilitati a presentare riesame (e quindi a sollecitare un controllo sula *lawfulness* del provvedimento), fra gli altri, anche i soggetti a cui spetta la restituzione del bene (art. 257 c.p.p.), che tendenzialmente non entrano nel mirino dell'inquirente (non sono, cioè, soggetti nei cui confronti la misura viene disposta). Il parallelo, a ben vedere, non regge: le intercettazioni insistono sulla persona; il sequestro, sulla *res*. E il rapporto privilegiato che chi ha diritto alla restituzione della cosa intrattiene con quest'ultima gli dà titolo per presentare l'impugnazione.

[21] Va da sé che si deve trattare di un terzo autenticamente "randomly affected"; là dove questi, pur non direttamente sottoposto a controllo, risulti tuttavia il reale bersaglio degli inquirenti – si pensi, a questo proposito, al fenomeno delle intercettazioni indirette (strumentali) dei membri del Parlamento di cui s'è molto discusso a margine di alcune importanti pronunce della Corte costituzionale (C. cost., sent. 23 novembre 2007 n. 390; C. cost., sent. 25 marzo 2010 n. 114; C. cost., sent. 28 dicembre 2023 n. 227) – la legittimazione si riespande.

Non solo: il criterio proposto vale a ricomprendere fra i soggetti abilitati ad azionare il costituendo rimedio anche coloro che, pur non essendo i titolari dell'utenza telefonica monitorata, ne sono gli effettivi utilizzatori (v. *supra*, par. 2, nota 13).

anche sulla legittimità dell'attività investigativa, e quindi sulla spendibilità processuale dei relativi risultati, costituisce, in certa misura, un'"invasione di campo". Le valutazioni sulla composizione del compendio probatorio subiscono l'influenza di chi a questa dinamica rimane estraneo (poiché non è parte) ed è portatore di interessi diversi. Da «convitato di pietra», la persona estranea al procedimento arriva ad acquisire uno spazio notevole, con il rischio di smottamenti e scompensi nel sistema[22]. Rischio – è banale dirlo – che cresce a dismisura se il rimedio si apre a "tutti i terzi"[23] presi in considerazione dall'art. 269, co. 2 c.p.p.

3. Possibili strade per un allineamento del diritto interno agli orizzonti europei: interpretazione convenzionalmente orientata dell'art. 269, co. 2 c.p.p.…

Una volta messo a fuoco quel che la Corte europea chiede (pur con i profili d'incertezza di cui s'è detto), è tempo di stringere lo sguardo sul diritto interno e ragionare sugli interventi necessari a colmare i deficit di tutela riscontrati.

Due sono le opzioni sul tavolo: da una parte, lavorare sull'esistente; dall'altra, costruire un rimedio *ex novo*.

La prima soluzione chiama in causa l'art. 269, co. 2 c.p.p. – il meccanismo azionabile (anche) dal terzo estraneo al procedimento a protezione dei propri diritti già presente nel sistema ma inadeguato allo sco-

[22] S. RENZETTI, *Una riforma (radicale?) per tornare allo spirito originario della legge: la nuova disciplina acquisitiva delle intercettazioni tra legalità, diritto vivente e* soft law, in *Leg. pen.* (rivista web), 4 aprile 2018, p. 67 ss. (ultimo accesso il 28 febbraio 2025).

[23] Chi è sottoposto a controllo dall'autorità, gli interlocutori degli intercettati e pure i soggetti citati nel corso dei colloqui (v. F. CAPRIOLI, *Intercettazioni e tutela della privacy nella cornice costituzionale*, in *Cass. pen.*, 2021, 4, p. 1151; S. COTRONEO, *La distruzione della documentazione relativa a intercettazioni* ex *art. 269 c.p.p.*, in *Giust. pen.*, 1999, III, c. 308). Sull'esigenza di interpretare con una certa elasticità la lettera dell'art. 269, co. 2 c.p.p. in ragione della «*ratio* dell'istituto, che costituisce un rimedio *ex post* alle formidabili capacità intrusive dell'intercettazione», v. A. CAMON, *Le intercettazioni nel processo penale*, Padova, 1996, p. 246 ss.

po[24] – e ne suggerisce una lettura correttiva. Si tratta, in sostanza, di aprire lo scrutinio del giudice anche ai profili che riguardano la legittimità della misura, profili che – è stato osservato – sono naturalmente ricompresi nel bilanciamento, invocato dalla norma, tra tutela della riservatezza (dell'interessato che chiede la distruzione dei colloqui) e istanze repressive (che militano in favore della conservazione): «tale giudizio sembra presupporre il preventivo superamento del vaglio di legittimità» della decisione genetica dell'attività investigativa. «Non avrebbe senso […] sofferma[rsi] sulla rilevanza […] di prove che fossero state acquisite in violazione dei divieti stabiliti dalla legge e, come tali, inutilizzabili»[25].

Imboccare la strada della lettura convenzionalmente orientata offre un chiaro vantaggio: consente di prescindere da un'iniziativa del legislatore (che allo stato peraltro pare fuori discussione)[26]. Ma è una strada impervia.

È senz'altro vero, infatti, che, se il giudice valuta la necessità di un'intercettazione ai fini del procedimento, deve aver risolto a monte la questione circa la legittimità della misura, e quindi l'utilizzabilità dei relativi risultati, ma questo non significa che il terzo, avvalendosi dello strumento offerto dall'art. 269, co. 2 c.p.p., abbia voce in capitolo. Quello spazio d'intervento è pensato per altro[27]: ottenere la distruzione di conversazioni utilizzabili (uscite indenni dalla procedura di selezione e pure dal "monitoraggio" del giudice *ex* art. 271 c.p.p.), ma scartate dalle parti perché ritenute (almeno fin lì) non rilevanti (quelle dotate di qualche interesse sul piano probatorio transitano nel fascicolo delle in-

[24] V. *supra*, par. 1.

[25] L. GIORDANO, *Considerazioni sulla sentenza della Cedu Contrada c. Italia n. 4*, cit.

[26] V. *infra*, par. 4.

[27] Contribuire a realizzare l'auspicio espresso dalla Corte costituzionale nella sentenza fondativa delle garanzie in materia di intercettazioni (C. cost., sent. 6 aprile 1973 n. 34) circa la costruzione di un «compiuto sistema – anche a garanzia di tutte le parti in causa – per l'eliminazione del materiale non pertinente». Così S. COTRONEO, *op. cit.*, c. 307. P. RIVELLO, *Il procedimento acquisitivo delle intercettazioni e l'archivio riservato presso il pubblico ministero*, in O. MAZZA (a cura di), *Le nuove intercettazioni*, Torino, 2018, p. 88, condivisibilmente rintraccia nel «diritto all'oblio» la radice profonda della disposizione.

dagini e poi in quello del dibattimento)[28]. È su questo materiale "di risulta" che si permette (anche)[29] al terzo coinvolto nelle attività di ascolto di interloquire a tutela della riservatezza[30].

Una conferma si ricava dalla lettera della legge: «*salvo quanto previsto dall'art. 271, comma 3*, le registrazioni sono conservate fino alla sentenza non più soggetta a impugnazione. Tuttavia gli interessati […] possono chiederne la distruzione»[31] (corsivo aggiunto). Il materiale sindacabile *ex* art. 269, co. 2 c.p.p. è quello conservato nell'archivio: tutte le registrazioni, al netto di quelle *contra legem*, che seguono l'apposita procedura di eliminazione nell'ambito della quale sono coinvolti solo il giudice e le parti. Che sia questa la corretta esegesi della clausola di salvezza, l'ha detto anche la Corte costituzionale. Nel risolvere il con-

[28] Nota R. ORLANDI (*Distruggete quelle intercettazioni!*, in *Cass pen.*, 2013, 4, p. 1355): quel che è in gioco nella procedura *ex* art. 269, co. 2 c.p.p. è «la distruzione di un mezzo di prova (legittimamente acquisito), inizialmente considerato irrilevante, ma che potrebbe rivelarsi rilevante per la parte che non ne conosceva l'esistenza e anche per l'altra, *re melius perpensa*». La prassi applicativa restituisce un'immagine aderente a questo schema. A meno che qualcosa non sia sfuggito, tutte le sentenze – poche, per verità – registrate nei repertori si riferiscono a richieste di distruzione motivate dalla ritenuta irrilevanza dei colloqui. V., da ultimo, Cass., sez. V, sent. 5 dicembre 2022 n. 10982, Macchi, in *CED Cass.*, n. 284672; Cass., sez. IV, sent. 23 settembre 2022 n. 43477, Livon, in *CED Cass.*, n. 283924.

[29] Nella categoria degli «interessati» rientrano anche le parti. V. S. RENZETTI, *Il percorso dei colloqui intercettati: dal brogliaccio alla prova*, in G. GIOSTRA, R. ORLANDI (a cura di), *Revisioni normative in tema di intercettazioni*, Torino, 2021, p. 87. Per verità, dubbi erano sorti in passato sulla legittimazione del pubblico ministero, ma la Corte costituzionale li ha risolutamente fugati (C. cost., sent. 30 dicembre 1994 n. 463). Del resto, «per ragioni ovvie – i suoi rapporti con la polizia; i suoi compiti di direzione dell'indagine – chi può accorgersi rapidamente della presenza agli atti di registrazioni irrilevanti è proprio il pubblico ministero», chiosa efficacemente A. CAMON, *Alcuni tratti della riforma*, in *Leg. pen.* (rivista web), 24 novembre 2020, p. 12, nota 39 (ultimo accesso il 28 febbraio 2025).

[30] Esclude che i soggetti estranei al procedimento siano «legittimi contraddittori» nella parentesi dialettica dedicata alla selezione delle intercettazioni utilizzabili, C. CONTI, *La riservatezza delle intercettazioni nella "delega Orlando"*, in *Diritto penale contemporaneo - Rivista trimestrale*, 2017, 3, p. 92 s. Condivide la linea S. RENZETTI, *Una riforma (radicale?) per tornare allo spirito originario della legge*, cit., p. 68.

[31] Vedi però L. GIORDANO (*Considerazioni sulla sentenza della Cedu Contrada c. Italia n. 4*, cit.), che legge l'inciso in senso diametralmente opposto.

flitto di attribuzione sorto a seguito dell'intercettazione casuale di alcune conversazioni dell'ex Presidente della Repubblica Giorgio Napolitano nell'ambito di un'indagine svolta dalla Procura di Palermo, la Consulta ha escluso che l'art. 269, co. 2 c.p.p. offrisse uno strumento utile a ottenere la distruzione dei colloqui riferibili dalla prima carica dello Stato, proprio perché, fra l'altro, la procedura

> riguarda per definizione conversazioni prive di rilevanza ma astrattamente utilizzabili, *come risulta dalla clausola di esclusione inserita, rispetto alle intercettazioni di cui sia vietata l'utilizzazione, in apertura del secondo comma dell'art. 269 c.p.p.*[32] (l'enfasi è nostra).

L'assetto ha una sua logica: il diritto alla prova prevale sul diritto alla riservatezza. La tutela della privacy è sacrosanta, ma pur sempre recessiva rispetto «al conseguimento del fine primario: la realizzazione di un processo giusto che assolva gli innocenti e condanni i colpevoli»[33].

Insomma, ci sono solidi motivi per ritenere che la lettura convenzionalmente orientata sia, nella sostanza, un'interpretazione *contra legem*, e quindi impraticabile; a ciò si aggiungono anche un paio di considerazioni pratiche.

La prima: l'idea di lavorare sull'esistente incontra un fattore di complicazione, se non proprio un limite, nella differente latitudine applicativa dei due rimedi, quello – più stretto[34] – preteso dalla Corte europea e quello ampio[35] già presente nel sistema. Ancora: val la pena metter mano alle norme perché, diversamente, rimarrebbe comunque scoperto il tema dell'avviso al terzo[36] – vero *punctum dolens* dell'art. 269, co. 2 c.p.p., all'origine di tutte le disfunzioni e inefficienze del meccanismo

[32] C. cost., 15 gennaio 2013, n. 1.

[33] G.P. VOENA, *Processo penale e mezzi di comunicazione di massa: un instabile stato dell'arte*, in *Processo penale e giustizia*, 2017, 6, p. 1125.

[34] L'osservazione coglie nel segno a patto che si condivida la ricostruzione, proposta nel paragrafo precedente, circa l'opportunità di restringere la legittimazione a contestare la legittimità della misura ai soli terzi direttamente intercettati.

[35] V. *supra*, par. 2, nt. 23.

[36] Lo sottolinea anche F.M. MANFRIN, *Le vite degli altri: Italia condannata per intercettazioni di terzi non indagati*, in *Riv. it. dir. proc. pen.*, 2024, 3, p. 1244.

ivi disciplinato[37]. Se ci limitassimo ad allargare il sindacato del giudice non risolveremmo il problema, e il risultato sarebbe che il congegno – anche nella sua versione estesa, in linea con i dettami di Strasburgo – continuerebbe a essere un «ramo secco dell'ordinamento»[38].

4. …o creazione di un rimedio ad hoc*?*

La prospettiva che punta alla modifica del quadro normativo per realizzare un rimedio nuovo e separato da quello che fa capo all'art. 269, co. 2 c.p.p. va coltivata dando conto, fin da subito, delle scarse possibilità di successo, quantomeno nel breve periodo. Dopo la condanna nel caso Contrada n. 4 il legislatore è intervenuto in materia di intercettazioni – di più, è intervenuto proprio sullo specifico tema della riservatezza dei terzi –, ma ha adottato soluzioni e accorgimenti che vanno in tutt'altra direzione[39]. Ha puntato ancora su modalità di protezione "indiretta" e passiva, mediante una stretta sulla diffusione delle informazioni riguardanti tali persone. In particolare, ha previsto che siano eclissate dai brogliacci (art. 268, co. 2-*bis*) e stralciate in fase di acquisizione (art. 268, co. 6) le espressioni «che consentono di identificare soggetti diversi dalle parti» (sempre che non ne sia provata la rilevanza); ha imposto modalità di tenuta dell'archivio *ex* art. 89-*bis* c.p.p. tali da garantire la segretezza, fra l'altro, della documentazione che riporta dati relativi a terzi (art. 89-*bis*, co. 2 disp. att.). Ancora: ha richiesto cautela in sede di confezionamento, rispettivamente della domanda e dell'ordinanza cautelare: anche qui, non c'è spazio per «dati personali dei soggetti diversi dalle parti, salvo che ciò sia indispensabile per la compiuta esposizione» dei fatti (artt. 291, co. 1-*ter* e 292, co. 2-*quater*)[40].

[37] V. *infra*, par. 4.

[38] A. CAMON, *Alcuni tratti della riforma*, cit., p. 12, nt. 39.

[39] L. 9 agosto 2024 n. 114, recante «Modifiche al codice penale, al codice di procedura penale, all'ordinamento giudiziario e al codice dell'ordinamento militare», in G.U., 10 agosto 2024 n. 187.

[40] La riforma Nordio sulle intercettazioni è stata analizzata, con varietà di accenti, da P. BRONZO, *Brevi note sul "disegno di legge Nordio"*, in *Sistema penale* (rivista web), 12 aprile 2024 (ultimo accesso il 28 febbraio 2025); G. ILLUMINATI, *Le modifiche al processo*

Ciò detto, e in attesa di vedere se la strategia alternativa messa in campo riuscirà indirettamente a colmare le lacune evidenziate a Strasburgo o se andremo incontro a condanne ancora più perentorie, val la pena mettere in fila alcune delle questioni – le più spinose, forse – che il legislatore dovrà affrontare se e quando deciderà di dar seguito al monito del giudice europeo.

L'avviso al terzo.

Lo dicono tutti, da sempre: se l'art. 269, co. 2 non funziona è perché le "vittime" della sorveglianza occulta diverse dalle parti, interessate a chiedere la distruzione del materiale raccolto dagli inquirenti, nella grande maggioranza dei casi nemmeno sanno d'essere state intercettate[41]. Se la volontà è quella di mettere a punto un rimedio effettivo, allora bisogna evitare di fare lo stesso errore. Tanto più che, diversamente da quello, il nuovo meccanismo non dovrebbe implicare oneri gravosi per il sistema. Se si accetta la tesi per cui i terzi abilitati sono soltanto i bersagli dell'attività investigativa, non si tratta di governare una moltitudine imponente di destinatari[42].

Sul punto, i primi commentatori hanno espresso opinioni discordanti: c'è chi[43] ha segnalato la necessità di prevedere forme di coinvolgi-

---

penale nel d.d.l. Nordio: una prima lettura, in *Riv. it. dir. proc. pen.*, 2023, 3, p. 886 ss.; F. DEMARTIS, *Intercettazioni: un correttivo che rafforza la riservatezza delle comunicazioni e tutela l'attività del difensore… ma scontenta i "curiosi"*, in *Dir. pen. proc.*, 2024, 9, p. 1168 ss.; L. FILIPPI, *Intercettazioni: un intervento legislativo all'insegna della tutela della* privacy, in G. SPANGHER (a cura di), *Il penalista. Le novità della legge Nordio*, 2024, Milano, p. 21 ss.; M. GIALUZ, *Le novità della "manovra Nordio" in materia processuale: quando l'ideologia rischia di provocare un'eterogenesi dei fini*, in *Sistema penale* (rivista web), 22 luglio 2024 (ultimo accesso il 28 febbraio 2025).

[41] V., fra i tanti, A. CAMON, *Forme, destinazione e regime della documentazione*, in G. GIOSTRA, R. ORLANDI (a cura di), *Nuove norme in materia di intercettazioni*, Torino, 2018, p. 91; G. GIOSTRA, *Intercettazioni fra indagini e* privacy, in *Dir. giust.*, 2006, 33, p. 99; S. RENZETTI, *Una riforma (radicale?) per tornare allo spirito originario della legge*, cit., p. 67.

[42] Insomma, non dovrebbe esserci il rischio di mettere in piedi soluzioni «praticamente impraticabil[i]». Così G. GIOSTRA, *La nuova tutela della* privacy *ovvero l'assai scadente traduzione giuridica di un proponimento condivisibile*, in *Sistema penale* (rivista web), 11 dicembre 2020, p. 5 (ultimo accesso il 28 febbraio 2025).

[43] E. SCORZA, *Diritto al rispetto della vita privata, procedimento penale e mezzi di ricerca della prova*, cit., p. 2851.

mento informativo del terzo, nella forma di una notifica *ex post*, o quantomeno un meccanismo di "informazione su richiesta", in linea con l'affermazione, assolutamente ricorrente nella giurisprudenza della Corte e presente anche nella sentenza Contrada n. 4 (al § 93), per cui

> la questione della notifica *a posteriori* di misure di sorveglianza è indissolubilmente legata a quella dell'effettività dei ricorsi giudiziari, e dunque all'esistenza di garanzie effettive contro gli abusi. La persona interessata non può, in linea di principio, contestare retrospettivamente dinanzi alla giustizia la legalità delle misure adottate a sua insaputa, a meno che non sia avvisata di queste ultime o salvo che – altro possibile scenario –, sospettando che le sue comunicazioni siano state sottoposte a intercettazione, la persona abbia [comunque] la facoltà di adire i tribunali.

Ma c'è anche chi[44] ha escluso tale scenario, facendo leva su altre affermazioni del giudice europeo; puntualizzazioni che immancabilmente accompagnano – e in certa misura stemperano – la sottolineatura del legame «indissolubile» che esiste tra comunicazione ed effettività del ricorso giudiziario. Si allude, in particolare, al rilievo secondo cui «l'esigenza della notifica successiva di una misura di intercettazione è legata a due fattori: la possibilità, nella pratica, di una tale notifica tenuto conto del contesto nel quale la sorveglianza è stata operata» e – qui arriva la chiosa sibillina – «se quest'ultima costituisca una condizione preliminare per avvalersi dei ricorsi giudiziari previsti dal diritto nazionale»[45].

A ben vedere, le ambiguità rilevate sono solo apparenti, e conseguenza della peculiare prospettiva – casistica e sviluppata in chiave retrospettiva – che connota il vaglio della Corte europea. Entro questa cornice, è chiaro che nell'ipotesi in cui un ricorso giurisdizionale sia previsto e risulti azionato, il tema del previo avviso finisce per passare in secondo piano ai fini del sindacato in ordine alla lamentata violazione dell'art. 8 Cedu. Ma se ci poniamo nell'ottica della costruzione d'un rimedio effettivo – un rimedio che metta l'interessato nella posizione di esercitare concretamente i propri diritti, anche di matrice sovranaziona-

[44] L. GIORDANO, *Considerazioni sulla sentenza della Cedu Contrada c. Italia n. 4*, cit.

[45] Corte eur. dir. uomo, sent. 23 maggio 2024, Contrada c. Italia (n. 4), sempre al § 93.

le –, la previsione di canali informativi a beneficio del terzo è imprescindibile.

A tal proposito, modelli (pur elaborati pensando all'esercizio delle prerogative di cui all'art. 269, co. 2 c.p.p.) a cui ispirarsi non mancano. Per esempio, la previsione d'un "avviso a persone non indagate", portata avanti dal d.d.l. Mastella dei primi anni Duemila[46]; oppure, l'idea, affacciatasi nella riflessione dottrinale[47], d'un meccanismo di conoscenza subordinato all'iniziativa dell'interessato.

Le modalità del coinvolgimento.

Per poter efficacemente contestare la legittimità della misura disposta nei suoi confronti, il terzo dovrebbe ovviamente avere accesso agli atti: decreti autorizzativi e verbali delle operazioni. C'è poi il nodo – assai intricato – relativo all'ascolto delle conversazioni. L'esigenza di acquisire contezza dei contenuti dei colloqui al fine di sollecitare il vaglio del giudice in maniera pienamente consapevole milita in favore dell'ingresso nelle sale d'ascolto, ma altri valori si oppongono recisamente a questo scenario: l'"amplificata" conoscenza delle intercettazioni, che inevitabilmente si determina quante più persone sono messe nella condizione di udire le registrazioni, viola la riservatezza di tutti i soggetti toccati dall'attività investigativa, *in primis* dell'imputato[48]. Il sistema prende seriamente in considerazione questo rischio; lo si ricava dalla lettera dell'art. 269, co. 1, in combinato disposto con l'art. 89-*bis* disp. att., che taglia fuori non solo i soggetti (anche terzi) che hanno

[46] Certo, andrebbe un poco affinata: per esempio, allargando il novero dei beneficiari dell'avviso oltre il perimetro dei titolari delle utenze telefoniche sottoposte a controllo. V. *supra*, par 2, nt. 21. Un'accurata fotografia delle opinioni suscitate dal disegno di legge – in tema di protezione della riservatezza dei terzi, ma non solo – è contenuta nella tavola rotonda (che vedeva fra i contraddittori L. FILIPPI, G. ILLUMINATI, G. LEO, P. PROFITI) ospitata da *Questione Giustizia*, 2006, 6, dal titolo *Quale riforma per la disciplina delle intercettazioni?*

[47] V. S. RENZETTI, *Una riforma (radicale?) per tornare allo spirito originario della legge*, cit., p. 71.

[48] È un cortocircuito per certi versi curioso: alla protezione della privacy del (singolo) terzo, linfa del vaglio giurisdizionale preteso da Strasburgo, si contrappone la protezione della privacy di (ogni) terzo (oltre che dell'imputato) finito "a portata di microspia".

diritto a chiedere la distruzione dei colloqui non necessari al procedimento, ma anche il rappresentante della persona offesa[49].

Prendere posizione in un senso o nell'altro è difficile; quel che si può ragionevolmente dire, però, è che, se il legislatore dovesse decidere di aprire al terzo le porte dell'archivio, dovrebbe imporre un ascolto necessariamente selettivo, limitato cioè ai singoli colloqui a lui riferibili.

Infine, i tempi del coinvolgimento.

Anche sotto questo profilo, contemperare tutti gli interessi in gioco non è semplice.

Il fatto che i terzi siano abilitati a interloquire sui presupposti della misura fa fisiologicamente arretrare le facoltà partecipative, le sospinge nella fase di acquisizione delle intercettazioni.

Non è una scelta obbligata, certo; si potrebbe pensare di aprire una finestra d'intervento successiva, mantenendo la procedura di selezione un "giardino proibito" solcato solo dalle parti e dal giudice. L'opzione tuttavia non è indolore, nella misura in cui mortifica le esigenze di economia processuale. A fronte dell'eccezione (posticipata) di illegittimità della misura, infatti, si dovrà giocoforza prevedere che il giudice fissi un'udienza in camera di consiglio per consentire a tutti gli interessati (*in primis*, le parti) di discuterne – in sostanza un'appendice, se non proprio una riedizione della procedura di stralcio. Entro questo schema, eventuali tentativi di riportare "a livello" il piatto della bilancia in cui si collocano le istanze di razionalizzazione ed efficienza sono destinati a generare scompensi d'altro tipo. Si pensi alla possibile costruzione d'una causa d'inammissibilità capace di "fulminare" le richieste integranti mera riproposizione di altre già presentate e decise in fase di selezione: il meccanismo ne uscirebbe in parte "alleggerito", ma il terzo, di fatto ammesso a interloquire solo sulle questioni che costituiscono un *novum*, vedrebbe schiacciati i suoi diritti d'intervento e partecipazione.

[49] V. Cass., sez. V, sent. 12 marzo 2021 n. 20639, Cafforio, in *CED Cass.*, n. 281257. Critica sul punto S. SIGNORATO, *L'archivio delle intercettazioni. La custodia del materiale e la marcia verso la digitalizzazione delle informazioni*, in *Leg. pen.* (rivista web), 24 novembre 2020, p. 86 (ultimo accesso il 28 febbraio 2025).

INDAGINI TECNOLOGICAMENTE ASSISTITE E TECNICHE INVESTIGATIVE SPECIALI

NOTE INTRODUTTIVE

Fabio Cassibba

In un recente articolo comparso sul New York Times, Mike Conley rammenta che le «persone non sono brave ad abbinare i volti. Le macchine invece sì, e soprattutto non si stancano».

Le due affermazioni, solo all'apparenza scontate, offrono una precisa chiave di lettura per introdurre l'odierna sessione di lavori. La prima – esprimendo un limite intrinseco alle capacità mnestiche delle persone – ben si presta a rappresentare il declino della prova dichiarativa nel processo penale, ormai marginalizzata a favore di esperimenti ad alto tasso tecnologico. La seconda – accattivante in una prospettiva efficientistica – trascura i rischi di un fideistico affidamento nelle tecnologie digitali, in grado di generare *output* falsamente positivi o negativi perché condizionati, fra l'altro, da *pattern* di informazioni iniziali erronee o incomplete.

Una premessa è indiscutibile: la società opera nel mondo digitale, comunica nel mondo digitale, talvolta "vive" (artificialmente, attraverso *avatar*) nel mondo digitale, lasciandovi innumerevoli e longeve tracce. Ovvio, dunque, che in quel mondo vengano inevitabilmente trascinate le investigazioni penali, compiute mediante strumenti tecnologicamente avanzati, sempre più sofisticati e subdoli in quanto capaci di una profonda e talvolta occulta (o difficilmente controllabile) attitudine intrusiva nei diritti fondamentali, ma non sempre rigidamente regolati da una precisa base legale.

Da qui, un inevitabile spostamento del baricentro del processo verso le indagini preliminari, per vero non ignorato dalla "Riforma Cartabia" che ambisce a rafforzare i poteri di controllo del giudice mediante la creazione di finestre giurisdizionali nel contesto che precede l'esercizio

dell'azione penale. Ma emerge al contempo una debolezza della manovra legislativa o – se si preferisce – un suo paradossale strabismo. Mentre la prova orale è in crisi, il legislatore si muove per irrobustire le forme di documentazione degli atti unilaterali a contenuto dichiarativo, con l'implicito intento – a ben vedere – di rendere maggiormente solida la base cognitiva per i riti alternativi. Tuttavia, analoghe scelte non si registrano sul terreno degli atti d'indagine "tecnologicamente assistiti", benché fosse assai avvertito il bisogno di un intervento normativo proprio là dove la prassi incide maggiormente. Si pensi all'aggiramento dei limiti normativi per l'impiego di prove "atipiche" o all'indebita estensione della categoria della prova documentale a tutto discapito delle tutele rafforzate accordate alla corrispondenza, nell'ampio (e, al contempo, ovvio) significato datole da C. cost., sent. 22 giugno 2023 n. 170, idoneo a includere anche la «messaggistica istantanea» veicolata dalle varie piattaforme *social*.

Occorre, allora, procedere a colmare i vuoti di tutela che ancora affliggono i diritti fondamentali *del* e *nel* processo, in special modo quando ne venga in gioco la dimensione digitale, attraverso una riforma sistematicamente coerente, fondata sui pilastri costituzionali e sovranazionali che sorreggono il diritto alla privatezza e quello alla libertà e alla segretezza delle comunicazioni.

Andrebbe recuperata appieno l'esigenza di determinatezza e tassatività degli esperimenti probatori, superando la disciplina racchiusa nell'art. 189 c.p.p., ormai logora e trasfigurata dalla prassi, che la impiega come grimaldello per scardinare la legalità processuale.

Inoltre, andrebbero espresse sul terreno normativo le generali implicazioni del principio di proporzionalità, volto a operare, *a priori*, come limite al compimento di atti d'indagine e, *a posteriori*, come criterio di ammissione probatoria o, se si preferisce, come regola di esclusione verso prove la cui raccolta abbia realizzato un'interferenza sproporzionata nei diritti fondamentali.

Infine, nella medesima prospettiva della necessaria valorizzazione del canone di proporzionalità, andrebbe decisamente irrobustito il ruolo del giudice per le indagini preliminari. Occorre ricondurre la figura del pubblico ministero al suo genuino ruolo di parte e, dunque, di organo "della domanda", privandolo del potere di autonomamente disporre atti

d'indagine fortemente intrusivi nei diritti fondamentali, salva l'ipotesi della stretta urgenza, incompatibile con la previa autorizzazione giurisdizionale, per cui resta comunque necessaria la tempestiva convalida del giudice. Il solco dei futuribili interventi normativi è, del resto, già tracciato dalla recente giurisprudenza della Corte di giustizia dell'Unione europea in ordine all'acquisizione dei "tabulati" e al previo controllo giurisdizionale sugli atti d'indagine *crossborder* compiuti dalla Procura europea.

Affinché il disegno riformatore assicuri una tutela effettiva ai diritti fondamentali, occorre però che il legislatore nazionale compia un passo coraggioso, svincolandosi dalle scelte di fondo che caratterizzavano l'assetto impresso alle indagini preliminari dal codice del 1988. Va superato l'assunto in forza del quale il controllo del giudice per le indagini preliminari è condizionato dal deposito di atti strategicamente e discrezionalmente selezionati dal pubblico ministero. Alla cognizione sommaria perché parziale del giudice per le indagini preliminari va sostituita una cognizione completa: al momento della richiesta di autorizzazione di un atto, il pubblico ministero dev'essere onerato dal deposito dell'intero compendio investigativo allestito, in difetto del quale resta privo di significato lo stesso controllo sulla proporzionalità.

Il già segnalato spostamento del baricentro procedimentale prima dell'esercizio dell'azione penale – dove si gioca l'autentica partita – e la centralità delle prove tecnologiche (e irripetibili) esigono un giudice per le indagini preliminari dotato di occhi penetranti e braccia robuste per arginare l'attività investigativa.

Un *caveat*. Occorre evitare di cedere a due tentazioni contrarie: l'acritica fiducia nella pretesa, intrinseca affidabilità della prova elaborata o raccolta mediante nuove tecnologie e un altrettanto acritico pregiudizio verso queste ultime. Del resto, già a metà degli anni Ottanta del secolo scorso, Giovanni Paolo Voena poneva in luce come costituisse una battaglia di retroguardia erigere barriere antistoriche all'impiego delle tecnologie nel processo penale e come invece occorresse governarle.

I SEQUESTRI DI *SMARTPHONE*, DISPOSITIVI INFORMATICI E MEMORIE DIGITALI

Elisa Lorenzetto

SOMMARIO: *1. Dal sequestro del contenitore al sequestro del contenuto. 2. Vuoti normativi e pericolo di inciampi. 3.* Key-words*: a) proporzionalità. 4. Segue: b) riservatezza. 5. Segue: c) integrità. 6. Il futuribile art. 254*-ter *c.p.p. 7. Il velo digitale.*

1. Dal sequestro del contenitore al sequestro del contenuto

Nell'intenso dibattito sui rapporti fra prova informatica e processo penale, divampato apertamente dopo che la l. 18 marzo 2008 n. 48, di ratifica ed esecuzione della Convenzione di Budapest sul *cybercrime*[1], ha inserito nel codice di rito disposizioni specifiche per le indagini digitali[2], il titolo qui prescelto – *I sequestri di* smartphone*, dispositivi informatici e memorie digitali* – potrebbe evocare un sentore tanto di familiarità quanto, al contempo, di manifesta incompiutezza.

[1] Per un commento organico, v. L. LUPÀRIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009. V. altresì M.L. DI BITONTO, A. VITALE, A. MACRILLÒ, A. BARBIERI, E. FORLANI, *La ratifica della Convenzione del Consiglio d'Europa sul cybercrime: profili processuali*, in *Diritto dell'Internet*, 2008, 5, p. 503 ss.; L. LUPÀRIA, *La ratifica della Convenzione CyberCrime del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc.*, 2008, p. 720 ss.

[2] Sul significato tecnico delle locuzioni "indagini digitali", "indagini informatiche", "indagini elettroniche" e "indagini cibernetiche", spesso impiegate come sinonimi ma corrispondenti a realtà differenti, v. S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 43 ss. In argomento, v. anche S. ATERNO, Digital forensics *(investigazioni informatiche)*, in *Digesto Pen.*, Agg., VIII, Torino, 2014, p. 217; M. PITTIRUTI, Digital evidence *e procedimento penale*, Torino, 2017; A. TESTAGUZZA, Digital forensics. *Informatica giuridica e processo penale*, Milano, 2014.

Certamente in esso si riflette, pressoché alla lettera, la denominazione del recente d.d.l. n. 806 del 19 luglio 2023 («Modifiche al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici, smartphone e memorie digitali»)[3]. Progetto confluito, previo assorbimento del concorrente d.d.l. n. 690 del 9 maggio 2023 (a sua volta riferito al sequestro di «strumenti elettronici»)[4], nella più aggiornata proposta di legge n. 1822, quest'ultima approvata dal Senato della Repubblica, il 10 aprile 2024, con intestazione nuova («Modifiche al codice di procedura penale in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali»), e ora in attesa di esame alla Camera dei deputati[5].

[3] D'iniziativa dei senatori Zanettin e Bongiorno, in *Atti Senato, XIX leg., Disegni di legge e relazioni, Documenti*, stampato n. 806, il relativo testo si compone dell'unico art. 1, volto all'inserimento nel codice di procedura penale del nuovo art. 254-*ter* («Sequestro di dispositivi e sistemi informatici, *smartphone* e memorie digitali»).

[4] D'iniziativa del senatore Scarpinato, in *Atti Senato, XIX leg., Disegni di legge e relazioni, Documenti*, stampato n. 690, anche il suo testo contiene l'unico art. 1, volto all'inserimento nel codice di procedura penale del nuovo art. 254-*ter* («Sequestro di uno strumento elettronico»).

[5] Assegnato alla II Commissione Giustizia in sede Referente il 17 aprile 2024, con esame in Commissione iniziato il 9 aprile 2025, l'articolato, in *Atti Camera, XIX leg., Disegni di legge e relazioni, Documenti*, stampato n. A.C. 1822, si compone dell'art. 1, volto all'inserimento nel codice di procedura penale del nuovo art. 254-*ter* («Sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute») nonché degli artt. 2 («Ulteriori modifiche al codice di procedura penale»), 3 («Modifica alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale») e 4 («Disposizione transitoria»). Sulla più recente versione del prospettato art. 254-*ter* c.p.p., v. G.M. BACCARI, *La Corte costituzionale torna a pronunciarsi sull'acquisizione dei messaggi WhatsApp*, in *Processo penale e giustizia*, 2024, 4, p. 882 ss.; S. DE FLAMMINEIS, *Le sfide della prova digitale: sequestri*, chat, *processo penale telematico e intelligenza artificiale*, in *sistemapenale.it* (rivista web), 8 marzo 2024 (ultimo accesso il 28 febbraio 2025); O. MURRO, *Sequestro dei dispositivi informatici: verso l'art. 254* ter *c.p.p.? Brevi note a margine del d.d.l. A.S. n. 806*, in *penaledp.it* (rivista web), 12 marzo 2024 (ultimo accesso il 28 febbraio 2025); EAD., *Prospettive in tema di sequestro dello* smartphone: *le novità approvate dal Senato*, in *Dir. pen. proc.*, 2024, p. 1619 ss. Per un'analisi comparata degli originari d.d.l. n. 690 e n. 806 (v. *supra*, nt. 3 e 4), v. A. CHELO, *Tanto tuonò che piovve: il nuovo sequestro di dispositivi informatici*, in

Scelte lessicali a parte, tra le quali è indubbia l'assonanza, ciò che ciascuna di quelle formulazioni, incluso il titolo del presente lavoro, non riesce a rappresentare interamente è l'oggetto di questo peculiare sequestro: il quale, stando alla composita rubrica, nella sua più recente configurazione, del possibile, futuro art. 254-*ter* c.p.p., di cui si prospetta l'introduzione, riguarderà non soltanto – testualmente – «dispositivi e sistemi informatici o telematici» o «memorie digitali», ma anche «dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute»[6].

Forse, allora, si converrà con la scelta di non mutuare un elenco così verboso e cacofonico nell'intitolazione di un saggio. Ciò nondimeno risulta altamente pregnante, e va anzi valorizzato, il significato della puntuale enunciazione normativa *in fieri*[7], con la quale, se l'innesto dell'art. 254-*ter* c.p.p. vedrà la luce, occorrerà presto familiarizzare.

È, infatti, risaputo come quello in discorso sia un tipo speciale di sequestro: nella prassi qualificato per brevità "informatico", esso è privo della fisicità che connota tradizionalmente l'oggetto del sequestro probatorio, in relazione al quale l'art. 253 c.p.p. definisce «cose» tanto il «corpo del reato» quanto le entità «pertinenti al reato necessarie per l'accertamento dei fatti». Nel sequestro probatorio informatico sono, viceversa, rarissime le ipotesi in cui a rilevare è propriamente la "cosa"

Penale Diritto e Procedura - Rivista trimestrale, 2024, n. 1, p. 29 ss.; K. LA REGINA, *Il sequestro dei dispositivi di archiviazione digitale*, *ivi*, 2023, n. 3, p. 429 ss.

[6] La voluminosa rubrica del futuro art. 254-*ter* c.p.p. farà concorrenza a quella, altrettanto estesa, dell'art. 415-*ter* c.p.p. («Scadenza dei termini per l'assunzione delle determinazioni inerenti all'esercizio dell'azione penale. Diritti e facoltà dell'indagato e della persona offesa») o dell'art. 628-*bis* c.p.p. («Richiesta per l'eliminazione degli effetti pregiudizievoli delle decisioni adottate in violazione della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali o dei Protocolli addizionali»), quasi assecondando una tendenza emersa particolarmente nella legislazione più recente, specie in occasione dell'innesto di previsioni regolatrici di materie precedute da vivaci travagli giurisprudenziali.

[7] Anche tenuto conto delle *Regole e raccomandazioni per la formulazione tecnica dei testi legislativi*, Circolare del Presidente del Senato, 20 aprile 2001, in *senato.it*: «Ogni precetto normativo contenuto nell'atto è formulato evitando qualsiasi ambiguità semantica e sintattica e rispettando, per quanto possibile, sia il principio della semplicità che quello della precisione» (par. 2, lett. b).

in senso materiale (il contenitore)[8], essendo, semmai, di interesse investigativo il *quid* "dematerializzato" che quella cosa racchiude (il contenuto)[9].

Quest'ultimo rimanda alla ben nota distinzione fra risultanze "analogiche" (documento tradizionale) e risultanze "digitali" (documento informatico), dove a fare la differenza è il metodo di incorporamento, digitale appunto, mediante il quale la rappresentazione di un fatto è fissata al supporto fisico[10]. Proprietà che rende l'elemento informatico trasferibile da un supporto all'altro e altamente manipolabile, a cagione della sua congenita fragilità.

Di qui, l'esigenza delle misure tecniche e delle cautele, imposte dalla citata l. n. 48 del 2008, tese ad assicurare la conservazione e la non alterazione dei dati: sin dal primo sopralluogo di polizia giudiziaria si privilegia, in particolare, la loro duplicazione immediata, con una procedura che garantisca «la conformità della copia all'originale e la sua immodificabilità» (art. 354, co. 2, secondo periodo, c.p.p.)[11], secondo una prescrizione esplicitamente ribadita per la peculiare fattispecie del sequestro di dati informatici presso fornitori di servizi informatici, te-

[8] Per esempio, per il rilievo delle impronte digitali (ispezioni: artt. 244 ss. c.p.p.; accertamenti e rilievi: art. 359 c.p.p.) o ai fini del riconoscimento di un determinato *device* (individuazione di cose: art. 361 c.p.p.; ricognizione di cose: art. 215 c.p.p.).

[9] In tema di sequestro informatico, v. D. CURTOTTI, *Il sequestro*, in AA.VV., Cyber forensic *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Torino, 2021, p. 457 ss.; A. TESTAGUZZA, *Il sequestro di dati e sistemi*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (diretto da), Cybercrime. *Trattato di diritto penale*, 2ª ed., Torino, 2023, p. 1643 ss. Per uno studio recente, specificamente riferito al dispositivo di telefonia mobile dotato delle potenzialità di un sistema informatico o telematico, v. O. MURRO, *Lo* smartphone *come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati*, Torino, 2024.

[10] La distinzione tra incorporamento analogico e digitale è tracciata da P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, p. 403 ss. V. inoltre ID., *L'evoluzione delle categorie tradizionali: il documento informatico*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (diretto da), Cybercrime. *Trattato di diritto penale*, cit., p. 1510, per la definizione di documento informatico quale «rappresentazione di un fatto che è incorporata con modalità digitali su di una base materiale».

[11] Sul tema, v. volendo E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in L. LUPÀRIA (a cura di), *Sistema penale e criminalità informatica*, cit., p. 135 ss.

lematici e di telecomunicazioni (art. 254-*bis* c.p.p.)[12]. Senonché, malgrado le assolute specificità di tutte le acquisizioni informatiche, di cui offrono traccia pure gli accorgimenti in materia di ispezioni e perquisizioni disposte dall'autorità giudiziaria (art. 244, co. 2, secondo periodo, e art. 247, co. 1-*bis* c.p.p.)[13], manca nel codice di rito una disciplina generale che regoli compiutamente il passaggio, delicatissimo, dal sequestro del "contenitore" fisico al sequestro del "contenuto" digitale[14].

2. Vuoti normativi e pericolo di inciampi

Simile lacuna, alla quale la proposta di legge pendente punta ora a porre rimedio, si pone peraltro all'origine di un insidioso effetto collaterale che la pratica non ha tardato a portare allo scoperto.

Più precisamente, è oramai acclarato come la duplicazione integrale dei dati (c.d. copia-clone o copia forense) ottenuta tramite rigorosa copiatura *bit to bit* (nota come *bit stream image*)[15], vale a dire la misura

[12] A proposito del sequestro di dati informatici presso un *service provider*, v. S. VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, in L. LUPÀRIA (a cura di), Internet provider *e giustizia penale*, Milano, 2012, p. 107 ss.

[13] Sull'argomento, v. D. CURTOTTI, *Attività di acquisizione della* digital evidence*: ispezioni, perquisizioni e accertamenti tecnici*, in AA.VV., Cyber forensic *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, cit., p. 439 ss.; P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (diretto da), Cybercrime*. Trattato di diritto penale*, cit., p. 1583 ss.

[14] Muovendo dalla constatazione per cui, di norma, i mezzi di ricerca della prova realizzano una sorta di progressione, in forza della quale le ispezioni e le perquisizioni precedono il sequestro, si è osservato come nelle investigazioni informatiche la successione risulti sovente invertita, dal momento che le ispezioni e le perquisizioni digitali sono svolte dopo che il *device* è stato sequestrato (così, K. LA REGINA, *Il sequestro dei dispositivi di archiviazione digitale*, cit., p. 429; S. SIGNORATO, *Le indagini digitali*, cit., p. 221): la stessa anomalia verrebbe, tuttavia, ridimensionata con la regolamentazione apposita del sequestro propriamente informatico, a norma del prospettato art. 254-*ter* c.p.p., derivandone una chiara distinzione tra il sequestro del contenitore (antecedente alle esplorazioni digitali) e il sequestro del contenuto (successivo alle esplorazioni digitali).

[15] Per un approfondimento degli aspetti tecnici, con gli opportuni rimandi bibliografici, v. S. SIGNORATO, *Le indagini digitali*, cit., p. 223 ss.

funzionale a garantire sia l'identità tra i dati originali e quelli copiati sia la loro genuinità, in concreto abbia finito per tramutarsi essa stessa nell'acquisizione indiscriminata di una mole esponenziale di elementi (dati, informazioni, programmi, comunicazioni e corrispondenza informatica), proprio perché costituiti dall'intero contenuto di un qualsiasi supporto sequestrato (dispositivi e sistemi informatici o telematici: *personal computer*, *tablet*, *smartphone*; memorie digitali: archivi USB, *hard-disk*)[16]. Situazione davvero insostenibile, sul piano della smisurata compressione delle garanzie fondamentali, e resa ancor più grave al cospetto dei dati digitali che veicolano contenuti propriamente comunicativi (SMS e MMS; messaggi di posta elettronica: *e-mail*; interazioni di varia natura mediante applicazioni di messaggistica istantanea: *chat*) per i quali i presidi sovraordinati e costituzionali si fanno più stringenti (art. 8 Cedu; art. 15 Cost.).

Se questo è il preoccupante assetto normativo vigente, va però dato atto che di quelle medesime istanze, inquadrabili nel rispetto del principio di proporzione[17] e nelle tutele che circondano la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione[18], si è resa portavoce autorevole la giurisprudenza di ogni livello – europea, costituzionale, di legittimità – imponendo un radicale adeguamento delle prassi. Tra queste ha fatto scuola la nota d'indirizzo organizzativo del 22 ottobre 2021, diramata dalla Procura Generale della Repubblica di Trento ai procuratori della Repubblica del distretto[19]. Alla stessa si de-

[16] Di qui, l'opinione secondo cui la copia forense, lungi dall'esaurirsi in una mera modalità di conservazione dei dati, costituirebbe essa stessa una forma di sequestro da assoggettare alla relativa disciplina: v. S. ATERNO, A. RAFFAELLI, Digital forensics *e* scena criminis, in D. CURTOTTI, L. SARAVO (a cura di), *Manuale delle investigazioni sulla scena del crimine*, 2ª ed., Torino, 2022, spec. p. 871 ss.; M. PITTIRUTI, Digital evidence *e procedimento penale*, cit., p. 38. Per una differente ricostruzione, favorevole a cogliere nella copia forense, anziché una modalità di sequestro, un autonomo atto investigativo di acquisizione di dati, perciò bisognoso di un intervento legislativo che ne detti una disciplina autonoma, v. S. SIGNORATO, *Le indagini digitali*, cit., p. 226 ss.

[17] V. *infra*, par. 3.

[18] V. *infra*, par. 4.

[19] Il cui testo è reperibile in *penaledp.it* (rivista web), 19 novembre 2021, con nota di L. FILIPPI, *Sequestro dei dispositivi elettronici: nota della Procura Generale di Trento* (ultimo accesso il 28 febbraio 2025).

ve, in particolare, l'indicazione della metrica ottimale da seguire per le acquisizioni digitali. Nell'ordine: *i*) sequestro del dispositivo; *ii*) copia forense della messaggistica e restituzione del dispositivo; *iii*) accertamento tecnico sulla copia forense, con selezione ed estrazione dei soli dati rilevanti ai fini dell'accertamento del reato per cui si procede (salva separata comunicazione di ogni notizia di reato diverso acquisita); *iv*) restituzione all'avente diritto della copia forense (e di ogni altra copia dei dati estratti dal dispositivo o relativa distruzione).

Dunque, una limpida successione di adempimenti distinti, in cui la copia-clone, come ha ben detto la Corte di legittimità, rappresenta il "mezzo" e non il "fine" del sequestro[20]. Proprio da simili basi il futuribile art. 254-*ter* c.p.p. ha preso, come si vedrà, più di uno spunto nel regolare la correlativa sequenza; e si è poi spinto addirittura lì, dove soltanto il legislatore sarebbe potuto arrivare: il riferimento è alla previsione, assolutamente innovativa, della garanzia giurisdizionale, prospettata sia per il preliminare sequestro dei "contenitori" (che si potrebbe definire sequestro-"mezzo", parafrasando il binomio coniato dai giudici di legittimità) sia per il successivo sequestro del "contenuto" (un sequestro-"fine") qualora si ricada nella specifica ipotesi dei dati aventi contenuto propriamente comunicativo.

Il punto sarà ripreso[21]. Per il momento, preme ancora evidenziare come l'approccio giurisprudenziale abbia, invece, mostrato assai minore sensibilità quando si è trattato di sindacare le concrete modalità operative che dovrebbero assicurare l'effettiva integrità degli elementi digitali acquisiti, con le dovute implicazioni quanto all'impiego delle risultanze[22]. Il tema chiama in causa le forme processuali da seguire in corrispondenza dello snodo a più elevato gradiente tecnologico – la copia forense – e le conseguenti, ipotetiche invalidità processuali, sulle quali dovrebbe incidere in primo luogo la possibilità di esercizio del contrad-

[20] Cfr. Cass. pen., sez. VI, sent. 22 settembre 2020 n. 34265, in *sistemapenale.it* (rivista web), 14 gennaio 2021, con nota di M. PITTIRUTI, *Dalla Corte di Cassazione un* vademecum *sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali* omnibus (ultimo accesso il 28 febbraio 2025).

[21] V. *infra*, par. 6.

[22] V. *infra*, par. 5.

dittorio. Tutte questioni rispetto alle quali, si vedrà, neppure il legislatore *in pectore* sembra offrire proposte originali né risolutive.

Facendo propria una tecnica di *computer forensics*, è dunque tramite le tre preannunciate parole-chiave – "proporzionalità", "riservatezza", "integrità" – che si darà ora brevemente conto dei connotati più controversi già affiorati nell'esperienza applicativa del sequestro informatico, ponendoli poi a confronto con il prodotto normativo in cantiere, allo scopo di coglierne gli aspetti perfettibili e le possibili rifrazioni sistematiche.

3. Key-words*: a) proporzionalità*

Muovendo dal primo connotato[23], certamente il sequestro informatico ha potuto beneficiare dei fondamentali approdi esegetici, maturati sulla scia delle pronunce europee in materia di misure limitative del diritto di proprietà[24], favorevoli a riconoscere l'estensione dei criteri di "proporzionalità", "adeguatezza" e "gradualità", previsti dall'art. 275

[23] Il canone di proporzione, nella sua triplice struttura (idoneità; stretta necessità; proporzionalità in senso stretto), può rivolgersi tanto al legislatore (proporzionalità in astratto) quanto all'interprete (proporzionalità in concreto): nel primo senso, si tratta di un criterio che orienta la formulazione delle fattispecie processuali, essendo, cioè, la legge a fissare presupposti, condizioni e limiti dell'ingerenza nella sfera dei diritti fondamentali; nel secondo senso, spetta agli operatori – segnatamente, all'autorità giudiziaria – effettuare il controllo di proporzionalità, sia nel momento in cui si valuta l'adozione di misure istruttorie foriere di siffatta ingerenza (controllo *ex ante*) sia nel momento in cui la valutazione così operata è sottoposta a verifica (controllo *ex post*). In argomento, v. M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Diritto penale contemporaneo - Rivista Trimestrale*, 2014, 3-4, p. 143 ss.; D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 2020, p. 3 ss. Per una disamina puntuale della sua incidenza applicativa nell'ambito del sequestro probatorio di materiale informatico, v. G. CASCONE, *Il sequestro informatico nel prisma del principio di proporzione*, in *Dir. pen. proc.*, 2022, p. 123 ss.

[24] V. Corte eur. dir. uomo, grande camera, sent. 5 gennaio 2000, Beyeler c. Italia; Corte eur. dir. uomo, sez. III, sent. 13 dicembre 2016, S.C. Fiercolect Impex S.r.l. c. Romania.

c.p.p. per la scelta delle misure cautelari personali, anche ai vincoli reali, di natura sia cautelare[25] sia probatoria[26].

Se ne è dedotto che il sequestro informatico, per le intrinseche peculiarità della copia-clone, che lo espongono al rischio di apprensione integrale della massa dei dati, debba soddisfare due precisi requisiti.

Per un verso, occorre un decreto di sequestro probatorio analiticamente motivato, cioè recante: *i*) le ragioni della necessità di un sequestro *ominubus* ovvero, in alternativa, delle specifiche informazioni oggetto di ricerca; *ii*) i criteri che devono presiedere alla selezione del materiale informatico archiviato nel dispositivo, giustificando, altresì, l'eventuale perimetrazione temporale dei dati di interesse in termini sensibilmente difformi dai confini temporali dell'imputazione provvisoria; *iii*) i tempi entro cui verrà effettuata tale selezione con conseguente restituzione anche della copia informatica dei dati non rilevanti[27].

Per altro verso, il sequestro si deve esplicare attraverso modalità operative coerenti con la natura servente della copia forense (copia-"mezzo" e non copia-"fine"), imponendosi, dopo la selezione dei dati, la restituzione del duplicato integrale il cui trattenimento finirebbe per eludere la prescritta necessarietà ai fini dell'accertamento del reato che, sola, legittima il sequestro probatorio *ex* art. 253, co. 1 c.p.p. Sono queste, avvertono i giudici di legittimità, le condizioni imprescindibili affinché il sequestro informatico non esondi in improprie finalità esplorative, cioè finalizzate «alla eventuale acquisizione, diretta o indiretta, di altre notizie di reato»[28].

I due moniti, come si vedrà, sono giunti forti e chiari al legislatore, che ne ha tentato il trapianto "in blocco" in quella disposizione da *re-*

[25] V. Cass. pen., sez. III, sent. 7 maggio 2014 n. 21271, Konovalov, in *CED Cass.*, n. 261509.

[26] V. Cass. pen., sez. un., sent. 19 aprile 2018 n. 36072, p.m. in proc. Botticelli, in *Dir. pen. proc.*, 2018, 10, p. 1263 ss.

[27] V. Cass. pen., sez. VI, sent. 22 settembre 2020 n. 34265, cit.; di recente, v. pure Cass. pen., sez. VI, sent. 15 febbraio 2024 n. 17312, Corsico, in *Giur. it.*, 2024, p. 2698 ss., con commento di D. CURTOTTI, *Brevi note in tema di proporzionalità del decreto di sequestro probatorio*, *ivi*, p. 2700 ss.

[28] V. Cass. pen., sez. VI, sent. 22 settembre 2020, n. 34265, cit.

cord – i commi programmati sono diciannove[29] – a cui potrebbe dare vita il futuro art. 254-*ter* c.p.p.[30].

4. Segue: b) riservatezza

Venendo al secondo connotato, è il potenziale contenuto comunicativo dei dati digitali a impattare il tema della riservatezza e delle garanzie connesse alla sua tutela. Materia che ha fatto registrare recenti e significativi avanzamenti, dei quali occorre fornire un pur breve richiamo[31].

Da una parte, è merito congiunto della Corte di giust. UE[32] e dello stesso legislatore domestico[33] se anche la procedura di acquisizione dei dati esterni di traffico telefonico e telematico (c.d. tabulati) richiede, ora, un provvedimento autorizzatorio motivato del giudice (oltre ai nuovi requisiti che ne circoscrivono il campo applicativo e la praticabilità). Si deve, invece, alla Corte costituzionale l'estensione alla corrispondenza elettronica della tutela offerta dall'art. 15 Cost., secondo un regime che si protrae anche dopo la ricezione da parte del destinatario,

[29] Quantità considerevole, tenuto conto che le *Regole e raccomandazioni per la formulazione tecnica dei testi legislativi*, Circolare del Presidente del Senato, 20 aprile 2001, cit., hanno cura di precisare: «È opportuno che ciascun articolo sia costituito da un numero limitato di commi» (par. 2, Raccomandazioni). Simile constatazione dovrebbe indurre a meditare sulla maggiore intellegibilità di una disciplina articolata in plurime disposizioni normative nonché, in più ampia prospettiva, sull'opportunità di sistematizzare l'intero complesso delle acquisizioni digitali in un comparto autonomo del codice di rito, onde superare l'attuale frammentarietà di una regolamentazione disseminata nelle progressive interpolazioni delle disposizioni preesistenti (sull'esperienza dell'ordinamento spagnolo, v. G. CASCONE, *La normativa spagnola in materia di misure di investigazione tecnologica nell'indagine penale: alcuni possibili spunti per il legislatore italiano per un approccio sistematico alla materia*, in *Cass. pen.*, 2023, p. 3006 ss.).

[30] V. *infra*, par. 6.

[31] Per i dettagli, v. in questo volume i contributi di A. CAMON, F. IOVENE e R. BELFIORE.

[32] V. CGUE, sent. 2 marzo 2021, causa C-746/18, H.K. c. Prokuratuur.

[33] V. art. 132 d.lgs. 30 giugno 2003 n. 196 (Codice Privacy), dopo la novella apportata con il d.l. 30 settembre 2021 n. 132, convertito con modificazioni dalla l. 23 novembre 2021 n. 178.

almeno fino a quando la corrispondenza «non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza»[34].

È vero, però, che i messaggi elettronici, a legislazione vigente, risultano acquisibili sulla scorta dell'art. 253 c.p.p. e secondo le apposite modalità stabilite dall'art. 254 c.p.p. per il sequestro di corrispondenza (presso i fornitori di servizi postali, telegrafici, telematici o di telecomunicazioni), escludendosi in particolare l'autorizzazione del giudice[35]. Nondimeno, il raffronto con la nuova disciplina di accesso ai dati "esterni" di traffico telefonico e telematico – lo evidenzia la stessa Corte costituzionale – andrebbe a rafforzare la conclusione per cui, a maggior ragione, per acquisire i "contenuti comunicativi" di quel traffico

[34] V. C. cost., sent. 27 luglio 2023 n. 170, in *penaledp.it* (rivista web), 6 settembre 2023, con nota di L. FILIPPI, *Il cellulare "contenitore" di corrispondenza anche se già letta dal destinatario* (ultimo accesso il 28 febbraio 2025), *ivi* e in *Penale Diritto e Procedura - Rivista trimestrale*, 2023, 3, p. 475 ss.; C. cost., sent. 28 dicembre 2023 n. 227, in *Processo penale e giustizia*, 2024, 4, p. 862 ss., con nota di G.M. BACCARI, *La Corte costituzionale torna a pronunciarsi sull'acquisizione dei messaggi WhatsApp*, cit., p. 877 ss. Per una ricaduta operativa, recentemente ravvisata dalla giurisprudenza di legittimità, v. Cass. pen., sez. VI, sent. 20 novembre 2024 n. 1269, in *CED Cass.*, n. 287504 – 01, secondo cui «(…) sono affetti da inutilizzabilità patologica i messaggi "*whatsapp*" acquisiti dalla polizia giudiziaria mediante "*screenshots*" eseguiti con il consenso dell'indagato, ma in mancanza degli avvisi delle facoltà difensive spettanti per l'apertura della corrispondenza, ivi compresa quella di rifiutare tale collaborazione, nonché del diritto di essere assistito da un difensore. (In motivazione, la Corte ha precisato che l'acquisizione di tale messaggistica con modalità non garantite non è consentita neppure quale prova atipica)». Per un commento, v. C. PARODI, *Acquisizione di* screenshot *da parte della P.G.: il consenso del proprietario del* device *non è sufficiente*, in *IUS Penale* (rivista web), 31 gennaio 2025 (ultimo accesso il 28 febbraio 2025). In altra occasione, la Cassazione ha decretato l'illegittimità dell'utilizzazione dei dati ottenuti mediante "ispezione telematica" di un cellulare dopo che il tribunale del riesame ne aveva annullato il sequestro: v. Cass. pen., sez. VI, sent. 21 maggio 2024 n. 31180, in *Cass. pen.*, 2024, p. 3417 ss., con commento di L. FILIPPI, *"Mettere il p.m. al suo posto" (ovvero la prova incostituzionale per* contempt of court *da parte del p.m.)*, *ivi*, p. 3424 ss.

[35] Nella giurisprudenza di merito, in favore dell'applicazione dell'art. 253 c.p.p. ed escludendo, segnatamente, la necessità dell'autorizzazione del giudice, v. Trib. Milano, sez. VII pen., ord. 5 dicembre 2023, in *giurisprudenzapenale.com* (rivista web), 11 dicembre 2023 (ultimo accesso il 28 febbraio 2025).

non sia più sufficiente il provvedimento del pubblico ministero, ma serva prevedere proprio l'autorizzazione del giudice[36].

Di qui, la peculiare disciplina riservata al sequestro dei dati comunicativi, della cui introduzione si fa carico l'art. 254-*ter* c.p.p., nei termini che si andranno a ricostruire[37].

5. Segue: c) integrità

Quanto al terzo e ultimo connotato, si può dire che l'integrità del dato digitale non sia mai stata percepita dalla giurisprudenza come un autentico elemento a rischio di compromissione nella fase acquisitiva.

Più in particolare, nelle massime riecheggia come un *mantra* l'assunto per cui le attività di estrazione di copia di *file* da *computer* non comportano attività di carattere valutativo su base tecnico-scientifica né

[36] Cfr. C. cost., sent. 27 luglio 2023 n. 170, cit., § 4.4: «Ma se, dunque, l'acquisizione dei dati esteriori di comunicazioni già avvenute (quali quelli memorizzati in un tabulato) gode delle tutele accordate dagli artt. 15 e 68, co. 3, cost., è impensabile che non ne fruisca, invece, il sequestro di messaggi elettronici, anche se già recapitati al destinatario: operazione che consente di venire a conoscenza non soltanto dei dati identificativi estrinseci delle comunicazioni, ma anche del loro contenuto, e dunque di attitudine intrusiva tendenzialmente maggiore». Nel senso di ritenere imprescindibile l'esigenza di un provvedimento autorizzativo di natura giurisdizionale, v. F. DINACCI, *I modi acquisitivi della messaggistica* chat *o* e-mail*: verso letture rispettose dei principi*, in *Archivio penale*, 2024, 1, p. 1 ss. In direzione ancora più netta, si segnala una recente pronuncia della Corte di Lussemburgo, per la quale il controllo preventivo di un giudice o di un'autorità indipendente si rende necessario ai fini dell'accesso ai dati personali (dunque, non soltanto ai contenuti comunicativi) presenti in un telefono cellulare, nel rispetto della direttiva 2016/680/UE del Parlamento europeo e del Consiglio, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati: v. CGUE, grande sezione, sent. 4 ottobre 2024, causa C-548/21, C.G., in *Cass. pen.*, 2025, p. 935 ss., con nota di P. DI STEFANO, *L'accesso ai fini di indagine ai dati contenuti in un telefono cellulare deve essere autorizzato dal giudice ed è consentito solo se l'ingerenza nei diritti fondamentali è proporzionata alle esigenze concrete dell'indagine penale*, *ivi*, p. 944 ss.

[37] V. *infra*, par. 6.

determinano alterazioni dello stato delle cose, tali da recare pregiudizio alla genuinità del contributo raccolto, essendo sempre possibile riprodurre informazioni identiche a quelle contenute nell'originale[38].

D'altro canto, stando ai principi già espressi dalla stessa Cassazione in materia di indagini informatiche, le norme di rilievo – quelle interpolate nel 2008 – non imporrebbero misure e procedure tipizzate, ma soltanto garanzie di conservazione e non alterazione dei dati (norme, per così dire, di scopo), tali da assicurare la conformità della copia all'originale e la sua immodificabilità[39]; mancando, inoltre, una sanzione processuale in caso di omessa adozione delle stesse cautele, le uniche conseguenze potrebbero prodursi sul piano dell'attendibilità della prova[40].

Intuibili i corollari: ampia discrezionalità del giudice nel valutare la prova (art. 192 c.p.p.) e onere a carico della difesa di dimostrare gli effetti deleteri per l'integrità dell'elemento acquisito.

Sul piano, invece, delle forme processuali da seguire – accertamento tecnico ripetibile (art. 359 c.p.p.) ovvero irripetibile (art. 360 c.p.p.) – si afferma che l'estrazione di dati archiviati in un *computer*, giovandosi di una tecnica che consente di acquisire il dato attraverso «operazioni meramente esecutive e materiali», senza necessità di perizia o consulenza, «non ha natura di accertamento tecnico irripetibile» ai sensi dell'art. 360 c.p.p.[41]. Sicché, la mancata adozione di tali modalità non comporta

---

[38] Principio sancito da Cass. pen., sez. I, sent. 5 marzo 2009 n. 14511, Aversano, in CED Cass., n. 243150; più di recente, v. Cass. pen., sez. III, sent. 5 aprile 2019 n. 42546, inedita; Cass. pen., sez. II, sent. 4 giugno 2015 n. 24998, in CED Cass., n. 264286. In termini critici rispetto all'esegesi prospettata in giurisprudenza, v. M. DANIELE, *Prova scientifica e regole di esclusione*, in G. CANZIO, L. LUPÀRIA (a cura di), *Prova scientifica e processo penale*, 2ª ed., Padova, 2022, p. 452.; ID., *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 297 ss.; L. MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4519 ss.; P. TONINI, *Considerazioni su diritto di difesa e prova scientifica*, in *Archivio penale*, 2011, p. 825 ss.; nonché, volendo, E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, p. 1530 ss.

[39] V. Cass. pen., sez. III, sent. 28 maggio 2015 n. 37644, in *CED Cass.*, n. 265180.

[40] V. Cass. pen., sez. V, sent. 16 novembre 2015 n. 11905/2016, Branchi, in *CED Cass.*, n. 265180.

[41] V. Cass. pen., sez. VI, sent. 20 dicembre 2018 n. 15838/2019, Viviano, in *CED Cass.*, n. 275541 – 01.

l'inutilizzabilità dei risultati probatori acquisiti, ma la necessità di valutare, in concreto, la sussistenza di eventuali alterazioni dei dati originali e la corrispondenza a essi di quelli estratti[42].

Tuttavia, e indipendentemente dalla circostanza che si agisca seguendo l'una o l'altra procedura[43], affinché la risultanza informatica sia utilmente acquisita occorre che in quelle sedi non sia stata prodotta alcuna alterazione, vale a dire che l'operatore abbia seguito un metodo affidabile, rispettoso delle linee guida di settore e fedele alla catena di custodia del reperto[44]. Profili, questi, sui quali dovrà potersi esercitare il contraddittorio: quanto meno *ex post* se l'acquisizione è stata eseguita in via unilaterale, quale forma di controllo differito circa la correttezza del metodo, l'integrità del dato e l'attendibilità della risultanza[45].

Sui medesimi aspetti, nondimeno, il futuribile art. 254-*ter* c.p.p. non prende una posizione davvero netta.

*6. Il futuribile art. 254-*ter *c.p.p.*

Entrando dunque nel merito del *novum* che si profila all'orizzonte, con l'innesto dell'art. 254-*ter* c.p.p. verrebbero, per la prima volta, declinate secondo una precisa scansione le singole fasi del sequestro in-

[42] V. Cass. pen., sez. III, sent. 8 luglio 2015 n. 29061, in *CED Cass.*, n. 264572.

[43] Nell'adozione della quale assume rilievo la circostanza che l'atto investigativo informatico sia compiuto su dispositivi spenti (*post mortem forensics*), configurandosi di regola come atto ripetibile (art. 359 c.p.p.), ovvero su dispositivi informatici trovati accesi (*live forensics*), nell'ambito dei quali molteplici dati sono destinati alla cancellazione qualora il dispositivo sia successivamente spento, qualificandosi le relative attività come accertamenti tecnici irripetibili poiché determinanti la modificazione irreversibile dei dati digitali (art. 360 c.p.p.; art. 117 disp. att. c.p.p.): cfr. S. SIGNORATO, *Le indagini digitali*, cit., p. 133 ss.

[44] Per un caso di violazione della catena di custodia, v. Cass. pen., sez. III, sent. 16 dicembre 2009 n. 2270, in *Dir. pen. proc.*, 2010, p. 1076.

[45] Secondo C. CONTI, *La prova informatica e il mancato rispetto della* best practice*: lineamenti sistematici sulle conseguenze processuali*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (diretto da), Cybercrime. *Trattato di diritto penale*, cit., p. 1532, «il contraddittorio, anche qualora venga attuato, non pone rimedio *di per sé* a eventuali vizi acquisitivi, dovuti al mancato rispetto delle corrette procedure» e, dunque, «il metodo dialettico non vale a esonerare dal rispetto della *best practice* di settore».

formatico, stabilendo per ciascuna competenze, presupposti e regole operative, nelle quali è percepibile l'eco delle tre parole-chiave – proporzionalità, riservatezza, integrità – emerse dall'esperienza applicativa.

Nel disegno del riformatore, l'*iter* ha inizio con il sequestro del contenitore (co. 1): si parla, segnatamente, «di dispositivi e sistemi informatici o telematici o di memorie digitali», che siano «necessari per la prosecuzione delle indagini in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto del principio di proporzione». La competenza, con una previsione assolutamente originale in raffronto all'assetto vigente, è assegnata al giudice per le indagini preliminari, il quale «a richiesta del pubblico ministero, dispone con decreto motivato il sequestro».

Non sono dettati limiti in relazione al reato per cui si procede (proporzionalità in astratto)[46]: semmai, la verifica di necessarietà (per la prosecuzione delle indagini) e di proporzionalità è affidata all'autorità giudiziaria (dunque, in concreto) e costituisce l'oggetto del preventivo controllo giudiziale, reso esplicito nel decreto motivato che testualmente "dispone" il sequestro (le intercettazioni e l'acquisizione dei tabulati sono invece "autorizzate": art. 267 c.p.p.; art. 132 d.lgs. n. 196 del 2003). Sicché vi è da credere che la richiesta del pubblico ministero dovrà essere corredata di elementi specifici affinché il vaglio del giudice possa rendersi effettivo. Quanto all'esecuzione del sequestro da parte del magistrato inquirente, la stessa deve avvenire «con modalità tecniche idonee a evitare l'alterazione o la perdita dei dati», ed è a tal fine che il pubblico ministero «adotta le misure tecniche necessarie o impartisce specifiche prescrizioni».

Tralasciando l'eventualità di una revoca del sequestro e la possibile adozione di una procedura d'urgenza, ipotesi appositamente regolate (co. 2, 3, 4 e 5), il secondo e autonomo *step* da compiersi si identifica propriamente con la copia forense (co. 6): il riferimento testuale è alla «duplicazione del contenuto dei dispositivi informatici, dei sistemi informatici o telematici o delle memorie digitali in sequestro», che dovrà, più in particolare, avvenire su adeguati supporti informatici mediante una procedura che assicuri «la conformità del duplicato all'originale e

[46] V. *supra*, nt. 23.

la sua immodificabilità» (co. 9) e sarà seguita dalla restituzione dei dispositivi all'avente diritto (co. 11).

Per realizzare la copia-clone il pubblico ministero sarà tenuto a instaurare il contraddittorio, sulla falsariga della disciplina dell'art. 360 c.p.p. (che tuttavia non viene richiamato)[47]: sono, infatti, previsti gli avvisi (alla persona sottoposta alle indagini, alla persona alla quale le cose sono state sequestrate e a quella che avrebbe diritto alla loro restituzione, alla persona offesa dal reato e ai relativi difensori) del giorno, dell'ora e del luogo per il conferimento dell'incarico per la duplicazione (con possibilità di parteciparvi a distanza: co. 7) e della facoltà di nominare consulenti tecnici (co. 6), i quali ultimi e i difensori potranno inoltre partecipare alle operazioni di duplicazione e formulare osservazioni o riserve (co. 8)[48]. Diversamente da quanto stabilisce l'art. 360 c.p.p., non è contemplata la riserva di incidente probatorio[49].

Peraltro, agli stessi adempimenti partecipativi si potrà derogare (co. 10): sia in presenza di reati gravi (oggetto di previsione mediante il richiamo ai procedimenti di cui agli artt. 406, co. 5-*bis* e art. 371-*bis*, co. 4-*bis* c.p.p.), a conferma di una concezione poco edificante del c.d. doppio binario (più rilevante è l'imputazione, meno rilevanti sono le garanzie); sia in caso di pericolo per la vita o l'incolumità di una persona o la sicurezza dello Stato; sia, ancora, se vi è pericolo di concreto pregiudizio per le indagini in corso o un pericolo attuale di cancellazione o dispersione dei dati (situazione nella quale potrebbe rientrare il caso del dispositivo trovato acceso che richiede, per motivi di carattere tecnico, un intervento rapido incompatibile con l'instaurazione del contraddittorio preventivo)[50].

---

[47] Un richiamo esplicito all'art. 360 c.p.p. era invece contenuto nel testo dell'art. 254-*ter* c.p.p. proposto dal d.d.l. n. 806 (v. *supra*, nt. 3).

[48] Sia pure riconoscendo che il d.d.l., «assai apprezzabilmente», introduce «una procedura di duplicazione "partecipata" dei contenuti del dispositivo», si osserva come il sistema risulti appesantito «da procedure macchinose di difficile concretizzazione pratica»: cfr. D. CURTOTTI, *Brevi note in tema di proporzionalità del decreto di sequestro probatorio*, cit., p. 2703.

[49] La relativa previsione (art. 360, co. 4 c.p.p.) veniva testualmente ritenuta non applicabile nella procedura delineata dall'art. 254-*ter* c.p.p. come prospettato dal d.d.l. n. 806 (v. *supra*, nt. 3).

[50] Sono i casi di *live forensics*: cfr. *supra*, nt. 43.

Seguirà, come terzo momento, l'analisi del duplicato, ultimata la quale si potrà procedere al vero e proprio sequestro del contenuto (co. 12), identificato come snodo autonomo e distinto dalla copia forense. A questo punto, l'*iter* incontra una fondamentale biforcazione, a seconda della natura (non comunicativa ovvero comunicativa) del materiale digitale: di norma, infatti, il pubblico ministero procede con decreto motivato al sequestro dei dati, dei programmi e delle informazioni, sempre a condizione che siano «strettamente pertinenti al reato in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto dei criteri di necessità e proporzione»[51]; viceversa, nello specifico caso di «dati inerenti a comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute», il pubblico ministero deve chiederne il sequestro al giudice per le indagini preliminari, che provvede con decreto motivato, disponendo il sequestro in presenza dei presupposti stabiliti per le intercettazioni (sono richiamati gli artt. 266, co. 1 e 267, co. l c.p.p., nonché l'art. 13 d.l. 13 maggio 1991 n. 152, convertito, con modificazioni, dalla l. 12 luglio 1991 n. 203)[52].

Tutti i dati sottoposti a sequestro sono quindi riversati su idonei supporti con modalità tecniche idonee ad assicurare la loro conformità ai medesimi dati contenuti nel duplicato e la loro immodificabilità (co. 13): una sorta, cioè, di copia-clone "ristretta", questa volta eseguita senza contraddittorio[53], che sarà acquisita al fascicolo, mentre la copia-clone

[51] Durante la gestazione della proposta di legge, si era auspicata l'introduzione di una procedura in contraddittorio davanti al giudice per lo stralcio dei dati irrilevanti, sulla falsariga di quella operante in materia di intercettazioni: v. K. LA REGINA, *Il sequestro dei dispositivi di archiviazione digitale*, cit., p. 432.

[52] In termini critici rispetto alla previsione che attribuisce «alla competenza del giudice solo il provvedimento iniziale di acquisizione massiva e indistinta» (cfr. co. 1), «restando il pubblico ministero il soggetto titolato al sequestro "definitivo" dei dati (non comunicativi) utili a fini di prova selezionati dal duplicato informatico» (cfr. co. 12), scelta che si porrebbe in potenziale contrasto con l'interpretazione di CGUE, grande sezione, sent. 4 ottobre 2024, causa C-548/21, C.G. (v. *supra*, nt. 36), cfr. P. DI STEFANO, *L'accesso ai fini di indagine ai dati contenuti in un telefono cellulare*, cit., p. 952.

[53] Dopo l'esercizio dell'azione penale, salvi i casi di cui all'art. 419, co. 3 c.p.p., il sequestro ai sensi dei co. 1 e 12 «è disposto dal giudice che procede» e, in tal caso, «alla duplicazione si procede con perizia»: co. 15 del futuribile art. 254-*ter* c.p.p.

"integrale" (cioè, il primo duplicato) sarà conservata presso la procura della Repubblica, protetta da misure di sicurezza e con modalità tali da assicurarne l'assoluta riservatezza (co. 16), sino alla pronuncia irrevocabile, fatta salva la facoltà degli interessati di chiedere la distruzione dei dati (co. 17)[54].

A completamento della disciplina, riconosciuta la possibilità di proporre riesame avverso tutti i provvedimenti di sequestro (del contenitore: co. 1; del contenuto: co. 12), nella disposizione *in fieri* manca una previsione esplicita di inutilizzabilità delle risultanze ottenute *contra legem* (vi è soltanto un richiamo all'art. 271 c.p.p.). Le ricadute pratiche saranno quelle già viste: ampia discrezionalità del giudice nel valutare la prova (art. 192 c.p.p.) e onere per la parte di dimostrare gli effetti deleteri per l'integrità dell'elemento acquisito. Onde contenere simili derive, si potrebbe replicare che un *deficit* tecnico nella copia forense genera una situazione di inidoneità probatoria sia del duplicato sia di ogni successiva analisi e sequestro condotti sullo stesso. A questo proposito, è vero che il requisito corrispondente – «essere idonea ad assicurare l'accertamento dei fatti» – costituisce parametro di ammissibilità della prova atipica (art. 189 c.p.p.), ma lo stesso può ritenersi presupposto implicito anche per l'ammissione di quella tipica[55]; e una prova inammissibile (art. 190 c.p.p.) non è utilizzabile (art. 191 c.p.p.)[56].

---

[54] Scelta anch'essa non soddisfacente, per il potenziale contrasto con la giurisprudenza di legittimità secondo la quale il duplicato del dispositivo informatico, una volta selezionato il materiale utile, deve essere restituito (v. *supra*, nt. 27 e 28), configurandosi altresì una disciplina che sembra orientarsi in direzione opposta al «principio di "minimizzazione dei dati", che dà espressione al principio di proporzionalità», come ribadito da CGUE, grande sezione, sent. 4 ottobre 2024, causa C-548/21, C.G., § 79, cit.: cfr. P. DI STEFANO, *L'accesso ai fini di indagine ai dati contenuti in un telefono cellulare*, cit., p. 952-953.

[55] Sul punto, v. C. BRUSCO, *La valutazione della prova scientifica*, in *Dir. pen. proc.*, 2008, supplemento al n. 6, p. 27.

[56] V. anche L. LUPÀRIA, *La disciplina processuale e le garanzie difensive*, in L. LUPÀRIA, G. ZICCARDI (a cura di), *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, p. 197, nel senso che il materiale raccolto sarebbe inutilizzabile per *unreliability*, vale a dire per inidoneità delle evidenze digitali ad assicurare un accertamento attendibile dei fatti di reato.

Va aggiunto, come spunto di futura riflessione, che manca pure ogni coordinamento rispetto alle investigazioni difensive (artt. 391-*bis* ss. c.p.p.), nell'ambito delle quali potrebbe presentarsi l'esigenza non tanto di "sequestrare" coattivamente i contenuti di un dispositivo informatico, quanto di acquisirli con modalità rituali ai fini della spendita nell'interesse dell'assistito (compresi la persona offesa e finanche un ente in previsione di un'ipotetica responsabilità ai sensi del d.lgs. 8 giugno 2001 n. 231). E in una materia, quali sono le indagini difensive, dove il principio di legalità viene spesso tradotto rigorosamente nella tassatività (nel senso che si ritiene il difensore legittimato a compiere soltanto le attività espressamente previste dal legislatore), un aggiornamento normativo potrebbe rendersi imprescindibile[57].

7. Il velo digitale

Nel protrarsi del dibattito in Parlamento, vi sarà tempo per valutare *funditus* la bontà della proposta normativa *in itinere*. Pur senza addentrarsi fra le singole asperità del prototipo in via di elaborazione, ma riguardando l'epopea del sequestro informatico nel suo complesso, sono due le linee di tendenza che si lasciano fin da subito intravedere.

Per un verso, si avverte il bisogno sia di un recupero della legalità in materia probatoria sia di un rafforzamento del ruolo del giudice in funzione di controllo e garanzia. In parallelo, però, proprio l'investitura del giudice a baluardo solitario della proporzionalità (in concreto) rischia di esonerare il legislatore dall'impegno nel dettare una disciplina puntuale di presupposti, condizioni e limiti del sequestro informatico, con un cortocircuito letale per la stessa legalità che si vorrebbe perseguire[58].

Resta ancora da chiedersi, a valle dell'*excursus*, quanto pesi oggi il velo digitale sulla pienezza di tutela dei diritti fondamentali attinti nelle

[57] A questo proposito, sia consentito il rinvio a E. LORENZETTO, *Il diritto di difendersi indagando nel sistema processuale penale*, Napoli, 2013, spec. p. 552 ss.

[58] V. nella stessa direzione le osservazioni di G. CASCONE, *Il sequestro informatico nel prisma del principio di proporzione*, cit., p. 137.

attività investigative[59]. Se, finora, il connotato tecnologico ha concorso al loro oscuramento, e le vicende della prova digitale ne costituiscono l'emblema[60], pare che il rischio stia ora profilandosi in prospettiva diametralmente opposta. Quasi che, al di fuori dello spettro delle investigazioni tecnologicamente assistite, la compressione dei diritti fondamentali non fosse ugualmente percepita: valga per tutti l'esempio della perquisizione domiciliare, certo non meno invasiva di un sequestro informatico, eppure non assistita dalla garanzia giurisdizionale; ma lo stesso potrebbe dirsi per il sequestro dei dati comunicativi analogici. Sarebbe, in definitiva, sorprendente e preoccupante se alla più ampia espansione dei diritti fondamentali finisse per porre un ostacolo, anziché il velo digitale, proprio la sua mancanza.

[59] Tema di rilievo anche ai fini della raccolta transnazionale della prova, come testimoniano le recenti pronunce della Corte di giustizia dell'Unione europea relativamente ai rimedi esperibili nello Stato di emissione dell'ordine europeo di indagine penale (CGUE, sent. 11 novembre 2021, causa C-852/19, Gavanozov); ai controlli giurisdizionali nelle indagini transfrontaliere della Procura europea (CGUE, grande sezione, sent. 21 dicembre 2023, causa C-281/22, G.K. e altri); ai dati di comunicazioni criptate acquisite mediante ordine europeo di indagine penale (CGUE, sent. 30 aprile 2024, causa C-670/22, M.N.). Per una ricostruzione sistematica della materia nello specifico campo delle acquisizioni digitali, v. G. DI PAOLO, *La circolazione transfrontaliera delle prove elettroniche*, in *Penale Diritto e Procedura - Rivista trimestrale*, 2024, 2, p. 265 ss.

[60] Ne offre una suggestiva anatomia L. LUPÀRIA, *La promessa della giustizia tecnologica*, in *sistemapenale.it* (rivista web), 1º agosto 2024 (ultimo accesso il 28 febbraio 2025).

LA GEOLOCALIZZAZIONE: TECNICHE E GARANZIE

Silvia Signorato

SOMMARIO: *1. Premessa: «Dove andiamo?». Scenari da* Panopticon*, tra cessione volontaria e dazione inconsapevole dei propri dati di localizzazione*. *2. Schizofrenia sistemica:* in medio stat virtus*. 3. Il pedinamento 'classico'* ex *art. 189 c.p.p. 4. La localizzazione satellitare non pare integrare una intercettazione e nemmeno un mezzo tipico di ricerca della prova. 5. La localizzazione satellitare quale forma di pedinamento elettronico, di regola meno invasivo del pedinamento 'classico'. 6. Controdeduzioni alla tesi dottrinale maggioritaria volta ad asserire la maggiore invasività della localizzazione satellitare rispetto al pedinamento. 7. Rifluenze dell'inquadramento giuridico della geolocalizzazione sulle attività captative oltre confine. 8. Segue: l'applicabilità dell'art. 234-*bis *c.p.p. e dell'art. 40 CAAS alla localizzazione satellitare all'estero. 9. I diritti in gioco nella localizzazione satellitare e nel pedinamento 'classico'. 10. Segue: riflessioni in tema di diritto al rispetto della vita privata e familiare* ex *art. 8 Cedu. 11. I dati di localizzazione dei tabulati. 12. Conclusioni: verso il superamento della parallasse percettiva nel bilanciamento delle garanzie.*

1. Premessa: «Dove andiamo?». Scenari da Panopticon*, tra cessione volontaria e dazione inconsapevole dei propri dati di localizzazione*

Nel 1897, in un periodo difficile della sua vita, segnato oltretutto dalla dolorosa perdita della figlia, Gauguin dipinse una tela dal titolo «Chi siamo? Da dove veniamo? *Dove andiamo?*». Si tratta di un'opera volta alla ricerca di un 'Oltre' che trascenda i limiti della ragione. Se la tecnologia non offre risposte alle questioni esistenziali indicate nel titolo dell'opera di Gauguin, nondimeno, essa è in grado di cristallizzare il «dove andiamo» quotidiano, monitorando gli spostamenti e delineando uno scenario ormai prossimo al *Panopticon*.

Invero, nella attuale società digitalizzata, molte persone acconsentono di continuo alla loro localizzazione da parte di terzi. Si pensi anzitutto alle situazioni in cui venga installato un dispositivo satellitare su un

veicolo al fine di fruire di una riduzione del premio R.C. auto[1] qualora il monitoraggio dei percorsi e della modalità di guida restituisca dati rassicuranti in rapporto alle garanzie assicurative. Inoltre, non possono essere dimenticati i casi in cui le persone accettino che venga individuata e utilizzata la loro ubicazione da parte di *app* che abbisognano di tali dati per offrire all'utente servizi quali l'indicazione degli itinerari da seguire, i percorsi caratterizzati dal minor tempo di percorrenza, le metropolitane o i mezzi da utilizzare per pervenire a una determinata meta, *etc.* In aggiunta, non sfugge come, sempre più spesso, le persone condividano con altri soggetti la propria ubicazione nei *social*. Non ci si riferisce tanto a commenti e foto dai quali si desume ove essi si trovino, quanto a tutte le ipotesi di condivisione della posizione, attraverso una apposita funzione prevista da vari *social*. Senza contare che, in taluni casi, è lo stesso legislatore a considerare la geolocalizzazione quale strumento di tutela delle persone, come emerge anche dall'art. 3 l. 17 maggio 2024 n. 70[2], che indica come criterio direttivo in materia di contrasto al bullismo e al cyberbullismo il «prevedere una specifica area dotata di una funzione di geolocalizzazione, attivabile previo consenso dell'utilizzatore».

Se, in simili evenienze, le persone sono di regola consapevoli di avere acconsentito all'uso dei propri dati di localizzazione, in molti altri lo ignorano o ne accettano soltanto il rischio, senza verificare se installando una determinata *app* accondiscendano anche al loro tracciamento e profilazione. Si consideri, poi, la localizzazione derivante dall'impiego del cellulare o il fatto che, non di rado, vengono indossati abiti dotati delle c.d. etichette intelligenti le quali, sfruttando la *Radio-Frequency Identification* (RFID), consentono entro certi limiti la localizzazione. Ancora, esiste tutta una serie di ulteriori possibilità tecnologiche di tracciamento. Senza addentrarsi negli aspetti tecnici, si ricordino soltanto *trasponder*, *Beacon*, etichette elettroniche con luce *led*, etc.

Invero, il sentire collettivo sembra caretterizzarsi per uno svilimento percettivo dei dati di localizzazione, tanto da accettare la loro trasmis-

[1] Il che è anche funzionale alla possibilità di essere in grado di dimostrare, in caso di targa clonata o di incidenti, dove si trovava realmente il proprio veicolo.

[2] Recante «Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo».

sione non solo al soggetto richiedente ma addirittura a terzi, pur di poter leggere gratuitamente un giornale o di fruire dei servizi offerti dalle *app*. Tant'è che, a livello statistico, la maggioranza delle persone non appare in grado di indicare il numero di coloro che tracciano i propri spostamenti, sembrando non accordare alcun rilievo a tale monitoraggio.

2. Schizofrenia sistemica: in medio stat virtus

A livello sistemico si assiste a una sorta di schizofrenia. Da un lato, infatti, i dati di localizzazione vengono percepiti come dati irrilevanti rispetto all'utilizzo di *app* o siti (che, oltretutto, utilizzano l'ubicazione a fini di profilazione), svelando un approccio collettivo, *in parte qua*, prevalentemente incurante della tutela della *privacy*; dall'altro lato, la sensibilità muta radicalmente allorché si tratti di acquisire i medesimi dati di localizzazione (senza successiva profilazione) in sede investigativa. In tal caso, i dati di tracciamento vengono considerati marcatamente lesivi della *privacy* al punto da invocare il presidio di ferree garanzie.

Qualcuno potrebbe forse sostenere che il diverso approccio sarebbe giustificato dal fatto che solo nel primo caso i dati di localizzazione vengono memorizzati e utilizzati in forza di un consenso, che è invece assente nel caso delle indagini. A una simile impostazione sarebbe però possibile obiettare su più fronti.

Anzitutto, è da dubitare che il consenso al monitoraggio degli spostamenti a fini di fruizione di servizi *internet* sia di regola un consenso espresso consapevolmente da parte degli utenti in rapporto alla incidenza sulla propria *privacy*; in molti casi, infatti, il consenso è prestato perché *conditio sine qua non* della fruibilità del servizio.

Inoltre, in rapporto alle indagini, vi è una base legale[3] in forza della quale si prescinde dal consenso in caso di trattamento di dati personali

[3] Il riferimento è alla Direttiva (UE) 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che

da parte delle autorità competenti per finalità investigative. Del resto, ben difficilmente un indagato presterebbe il consenso al trattamento di dati che possano essere utilizzati *contra se*, senza contare che la previa conoscenza dell'attività di monitoraggio degli spostamenti potrebbe determinare un cambio di itinerario[4], vanificando l'efficacia delle indagini.

In aggiunta, occorre verificare i diritti che vengono in rilievo. Nel caso di consenso più o meno consapevole a fini di fruizione di siti o *app* si rinuncia alla propria *privacy* per servizi anche non essenziali (ludici, estetici, fotografici, *etc.*). Invece, nel caso della localizzazione a scopo investigativo, il trattamento dei dati di ubicazione avviene anzitutto per assicurare l'attuazione dell'art. 112 Cost. Ciò non implica che il fine giustifichi i mezzi, ma che è necessario graduare con attenzione le garanzie pervenendo a un rapporto di equilibrio tra le stesse.

Come si esaminerà *infra* (par. 12) non si tratta di calibrare soltanto *privacy* e sicurezza, ma un ben più ampio ventaglio di tutele. Il che non può avvenire in maniera aritmetica, ma effettuando un bilanciamento tra i diritti, soppesandone adeguatamente le prevalenze, e ricercando la «medietà» secondo l'aristotelica Etica nicomachea, vale a dire individuando una disciplina delle garanzie che «né eccede né difetta»[5].

abroga la decisione quadro 2008/977/GAI del Consiglio; tale direttiva è stata attuata dal d.lgs. 18 maggio 2018 n. 51.

[4] Come rilevato da C. FANUELE, *La localizzazione satellitare nelle investigazioni penali*, Milano, 2019, p. 7, «l'utilità del 'seguire osservando' dipende esclusivamente dall'inconsapevolezza del soggetto».

[5] Cfr. ARISTOTELE, *Etica nicomachea*, 1106a, ove si legge: «chiamo medio della cosa il punto che dista ugualmente da ciascuno dei due estremi, punto che è unico e identico per tutti; chiamo invece medio rispetto a noi ciò che né eccede né difetta».

3. Il pedinamento 'classico' ex *art. 189 c.p.p.*

La tecnologia ha svelato nuove possibilità di localizzazione[6]. Il che ha posto dei problemi di inquadramento sistematico, dato che la disciplina in materia appare caratterizzata da aritmie e asimmetrie.

Infatti, per un verso, le varie modalità di localizzazione sono state disciplinate solo in alcuni casi; per altro verso, a seconda della tipologia di tracciamento, sussistono garanzie diverse a causa dell'applicabilità di istituti giuridici differenti (prove atipiche, c.d. tabulati, documenti, consulenza tecnica), senza contare che la tecnologia evolve, ponendo di continuo nuove questioni giuridiche.

Per comprenderle sembra opportuno muovere da un'analisi diacronica, ricordando che la prima tipologia investigativa volta alla localizzazione è rappresentata dal pedinamento. Si tratta di una indagine che dottrina e giurisprudenza del tutto maggioritarie hanno ricondotto alle investigazioni liberamente svolgibili dalla polizia giudiziaria ai sensi degli artt. 55 e 348 c.p.p. o, al più, ai sensi dell'art. 189 c.p.p.

Semmai, il dibattito si è incentrato sulla ripetibilità o irripetibilità del pedinamento, quale eco della riflessione dottrinale sul concetto di irripetibilità[7]. A livello giurisprudenziale, appare minoritaria l'impostazione secondo la quale il pedinamento sfuggirebbe alla disciplina prevista dall'art. 431, co. 1, lett. *b*, c.p.p. poiché la relativa documentazione potrebbe essere sostituita dalla rievocazione testimoniale da parte della polizia giudiziaria[8]. Invero, il pedinamento appare a tutti gli effetti una attività irrepetibile, con conseguente confluibilità dei relativi verbali nel fascicolo del dibattimento[9].

---

[6] Si pensi, per esempio, al c.d. IMSI *catcher*. In tema, cfr. W. NOCERINO, *Il tramonto dei mezzi di ricerca della prova nell'era 2.0*, in AA.VV., *Nuove tecnologie e processo penale*, Milano, 2021, p. 64 ss.

[7] Al riguardo, per tutti, cfr. C. CESARI, *L'irripetibilità sopravvenuta degli atti di indagine*, Milano, 1999.

[8] Per questa impostazione, si veda Cass. pen., sez. VI, sent. 8 giugno 2004 n. 39230, A., in *CED Cass.*, n. 230375 – 01.

[9] Al riguardo si veda Cass. pen., sez. III, sent. 9 novembre 2011 n. 44413, in *CED Cass.*, n. 251613 – 01, secondo la quale «Sono atti irripetibili, come tali acquisibili al fascicolo per il dibattimento, i verbali di pedinamento e appostamento della Polizia Giudiziaria».

Non sfugge, peraltro, come nella prassi investigativa venga talora redatta una mera annotazione e non sia così frequente l'inclusione di un verbale di pedinamento nel fascicolo del dibattimento.

4. La localizzazione satellitare non pare integrare una intercettazione e nemmeno un mezzo tipico di ricerca della prova

Se la riflessione dottrinale e giurisprudenziale in tema di pedinamento si è tendenzialmente incentrata sulla ripetibilità o irripetibilità dell'indagine, non si può dire lo stesso per la c.d. localizzazione GPS, dato che il suo utilizzo ha sollevato numerose questioni giuridiche.

Prima di esaminarle occorre effettuare una precisazione di carattere terminologico poiché i giuristi tendono a denominare 'localizzazione GPS' qualsiasi attività di individuazione della posizione che impieghi il segnale satellitare (ovvero la stessa tecnologia che utilizzano anche taluni navigatori delle auto). Invero, l'americano GPS è solo uno dei possibili gruppi di satelliti che emettono un segnale utile al monitoraggio; infatti, esistono molte altre costellazioni, tra cui la russa Glonass, la cinese BeiDou, l'europea Galileo. Per questo motivo, sarebbe più preciso non impiegare l'acronimo GPS, ma denominare l'indagine *tout court* come 'localizzazione satellitare'[10].

Sotto altro profilo, occorre essere consapevoli che, da un punto di vista tecnico, l'apparecchio che consente la localizzazione satellitare consta di due sottosistemi: un primo, tramite un algoritmo, calcola la posizione sulla base dei segnali radio che emettono i satelliti; un secondo, trasmette invece la posizione a un *device* degli investigatori, i quali

[10] Si può ricordare come la localizzazione satellitare sia anche alla base del funzionamento di taluni braccialetti elettronici. Al riguardo, cfr. P. SPAGNOLO, *Per un'effettiva gradualità delle misure cautelari personali*, in *LP*, 2014, 4, p. 335, nt. 8; E. VALENTINI, *Arresti domiciliari e indisponibilità del braccialetto elettronico: è il momento delle Sezioni Unite*, in *Diritto penale contemporaneo* (rivista web), 27 aprile 2016, p. 5, nota 13 (ultimo accesso il 28 febbraio 2025); nonché F. MENDITTO, *Ancora sul braccialetto elettronico e sull'art. 7 d.l. n. 178/2024*, in *Sistema penale* (rivista web), 19 dicembre 2024, che rileva però anche problemi applicativi (ultimo accesso il 28 febbraio 2025).

possono visualizzare una mappa cartografica degli spostamenti. Si noti che, di regola, la seconda fase (vale a dire la trasmissione alla polizia giudiziaria) non impiega alcun segnale satellitare, sfruttando invece altre tecnologie[11].

Ciò premesso occorre interrogarsi su quale tipologia investigativa integri la localizzazione satellitare[12].

Iniziando dalle esclusioni, anzitutto non pare si versi in una ipotesi di ispezione, ancorché elettronica. Infatti, diversamente da quanto previsto dall'art. 244 co. 1 c.p.p., la localizzazione non mira ad «accertare le tracce e gli altri effetti materiali del reato»[13]. Nemmeno essa sembra riconducibile entro il perimetro dei rilievi descrittivi *ex* art. 244 co. 2 c.p.p., i quali insistono su realtà che preesistono agli stessi, mentre il monitoraggio satellitare è sincronico. Ciò induce a escludere anche la riconducibilità di tale atto investigativo all'alveo degli accertamenti urgenti ai sensi dell'art. 354 c.p.p., senza contare che la localizzazione non è un'attività che mira a conservare «le cose, le tracce e i luoghi» né si esplica in «accertamenti e rilievi sullo stato dei luoghi e delle cose». Ancora, non sembra nemmeno ricorrere l'ipotesi prevista dall'art. 359 c.p.p., dato che la localizzazione non «implica una sintassi»[14], che è invece il presupposto dell'accertamento. In aggiunta, la localizzazione satellitare non può essere qualificata in termini di documento ai sensi dell'art. 234 c.p.p., poiché essa è un'attività investigativa (la relativa mappa cartografica rappresenta la sua documentazione), mentre il documento è una prova precostituita esterna all'attività investigativa[15].

---

[11] Per esempio, onde radio attraverso la rete locale *Global System for Mobile Communication* (GSM) o la rete *Global Packet Radio Service* (GSM/GPRS).

[12] Per una più compiuta e analitica ricostruzione al riguardo, sia consentito rinviare a S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. dir. process.*, 2012, pp. 583-587.

[13] Al contrario, evidenzia la vicinanza alle ispezioni per l'*inspicere*, l'esigenza documentativa e la possibilità di impiegare strumentazione tecnica, L. CARLI, *Le indagini preliminari nel sistema penale*, II ed., Milano, 2005, p. 33.

[14] In questi termini, in rapporto al concetto di accertamento, cfr. R.E. KOSTORIS, *I consulenti tecnici nel processo penale*, Milano, 1993, p. 138 ss.

[15] Cfr. *Relazione al progetto preliminare del c.p.p.*, in G.U., *Supplemento ordinario*, n. 2, 24 ottobre 1988, *Serie Generale*, p. 67, nonché L. KALB, *Il documento nel sistema probatorio*, Torino, 2000, p. 113.

Più delicato il tema della possibile riconduzione della localizzazione satellitare all'istituto delle intercettazioni. Secondo un orientamento, una simile eventualità andrebbe esclusa[16] perché la localizzazione non capterebbe alcuna comunicazione tra due soggetti. Se si condivide il punto di arrivo e, quindi, il fatto che la localizzazione satellitare non integra una intercettazione, sembra possibile inserire nel percorso argomentativo un ulteriore fattore, che fa leva sul concetto di riservatezza. Invero, al di là del fatto che non sembra sussistere alcuna comunicazione, vi è un aspetto tecnico che appare dirimente sul piano giuridico. L'intercettazione presuppone la captazione di un segnale riservato. Diversamente, la localizzazione capta un segnale aperto a tutti, tant'è che se ne può avvalere chiunque disponga di un navigatore.

Un ulteriore *punctum dolens* è rappresentato dalla possibilità di far confluire la disciplina della localizzazione satellitare in quella dei c.d. tabulati, *ex* art. 132 codice *privacy*[17]. Tuttavia, una simile opzione interpretativa non sembra poter essere accolta perché con la localizzazione satellitare non si capta alcuna comunicazione. Sicché appare del tutto condivisibile la tesi affermata dal Garante per la protezione dei dati personali, secondo il quale i dati di localizzazione acquisiti nell'ambito delle attività di polizia giudiziaria non possono essere definiti in termini di dati di traffico quando prescindono da una comunicazione[18].

---

[16] Per questa impostazione, si veda anche G. ILLUMINATI, *Libertà e segretezza della comunicazione*, in *Cass. pen.*, 2019, 11, p. 3832, che rimarca come la localizzazione satellitare integri un pedinamento elettronico.

[17] Come noto, si tratta del d.lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali).

[18] Al riguardo, si veda GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento 19 dicembre 2008*, relativo alla localizzazione delle persone disperse in montagna. Per il rilievo che i dati di localizzazione vengono captati in tempo reale a differenza di quanto previsto dalla disciplina *ex* art. 132 codice *privacy* che consente «l'accesso a dati preesistenti» si veda G. DI PAOLO, *Acquisizione dinamica dei dati relativi all'ubicazione del cellulare e altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense*, in R.E. KOSTORIS (atti raccolti da, con la collaborazione di C. BORTOLIN), *Le intercettazioni di conversazioni e comunicazioni. Per un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti. Atti del convegno dell'Associazione tra gli studiosi del processo penale "G.D. Pisapia"*, Milano, 2009, p. 233; nonché W. NOCERINO, *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio*, Milano, 2019, p. 131, nt. 130; S. MAR-

5. La localizzazione satellitare quale forma di pedinamento elettronico, di regola meno invasivo del pedinamento 'classico'

Al fine dell'inquadramento giuridico della localizzazione satellitare è bene muovere dalle fonti.

Al riguardo, occorre precisare come in seno al codice di procedura penale non vi sia alcuna norma che disciplini espressamente tale localizzazione.

Nondimeno, se si allarga l'orizzonte, si rinvengono delle previsioni che la qualificano in termini di 'pedinamento elettronico'[19]. In questa cornice si collocano ad esempio sia la l. 7 aprile 2011 n. 60[20] ove si fa espresso riferimento ai «mezzi tecnici, necessari per l'effettuazione (…) del *pedinamento*», sia il d.m. 1º dicembre 2010 n. 269[21], che annovera tra le attività svolgibili dai servizi di investigazione privata pure l'«attività di osservazione statica e dinamica (c.d. *pedinamento*) anche a mezzo di *strumenti elettronici*». Da ultimo, poi, anche un Documento del Senato impiega la locuzione «*pedinamento elettronico*»[22].

Dal canto suo, pure la giurisprudenza pressoché costante riconduce la localizzazione satellitare nell'alveo del pedinamento c.d. elettronico[23] e ritiene applicabile ad essa la disciplina prevista dall'art. 189 c.p.p.[24].

COLINI, *L'istituto della* data retention *tra legalità interna e internazionale*, in A. CADOPPI et al., *Cybercrime*, II ed., Torino, 2023, p. 1851.

[19] Come evidenziato da G. DI PAOLO, *'Tecnologie del controllo' e prova penale. L'esperienza statunitense e spunti per la comparazione*, Padova, 2008, p. 160, «il mutamento terminologico riflette l'intreccio tra la funzione tradizionale, rimasta inalterata, e le nuove modalità esecutive, ad alto contenuto tecnologico».

[20] Il riferimento è alla parte seconda, art. 6, co. 5, lett. i), lett. a.VI), della legge di ratifica ed esecuzione dell'Accordo tra il Governo della Repubblica italiana e il Governo della Repubblica di Slovenia sulla cooperazione transfrontaliera di polizia, fatto a Lubiana il 27 agosto 2007.

[21] Cfr. art. 5, co. 1, lett. a.VI).

[22] Si veda SENATO DELLA REPUBBLICA, *Documento approvato dalla 2ª Commissione permanente (Giustizia) nella seduta del 20 settembre 2023 a conclusione dell'indagine conoscitiva sul tema delle intercettazioni*, 2023, p. 38.

[23] *Ex multis*, cfr. Cass. pen., sez. II, sent. 18 settembre 2024 n. 37395, B., in *CED Cass.*, n. 286949 – 01.

[24] Secondo la *Relazione al progetto preliminare del codice di procedura penale*, a cura della commissione presieduta dal prof. Gian Domenico Pisapia, in G.U., 24 ottobre

A parere di chi scrive, in assenza di una disciplina *ad hoc* (che sarebbe comunque auspicabile, se non altro nel quadro di una più ampia riforma dell'art. 189 c.p.p.), la localizzazione satellitare può essere a tutti gli effetti qualificata in termini di pedinamento, essendo a essa accomunata dalla finalità del monitoraggio degli spostamenti e da una incidenza sui diritti fondamentali di regola *minore* rispetto al pedinamento 'classico'[25].

Poiché quest'ultima affermazione appare del tutto isolata in dottrina, sembra opportuno soffermarsi su di essa per sottoporre tale tesi al vaglio critico del lettore.

1988 n. 250, *Suppl. ord*. n. 93, *sub* art. 189 c.p.p., il codice avrebbe previsto l'art. 189 c.p.p. proprio per far fronte al «continuo sviluppo tecnologico che estende le frontiere dell'investigazione». In ogni caso, tale norma non potrebbe essere invocata per aggirare le garanzie e per il compimento di atti tipici *contra legem*. In questo senso, cfr. T. RAFARACI, *Ricognizione informale dell'imputato e (pretesa) fungibilità delle forme probatorie*, in *Cass. pen.*, 1998, p. 1741. Evidenzia come, nella prassi, si sia invece finito per legittimare prove irrituali facendo leva sul grimaldello dell'art. 189 c.p.p., O. MAZZA, *Critica delle prove atipiche nella deriva giurisprudenziale*, in *Diritto di Difesa*, 2022, 1, p. 64.

[25] Si può ricordare che, al di là della localizzazione come attività investigativa in sé, la giurisprudenza si è trovata a interrogarsi anche su questioni sempre nuove in tema di tracciamento. Ad esempio, si è chiesta se il reato di furto potesse dirsi consumato nonostante sul cellulare fosse installata una *app* in grado di localizzare lo *smartphone*, decidendo in senso positivo (al riguardo, si veda Cass. pen., sez. V, sent. 8 febbraio 2023 n. 12534), sul presupposto che nel tempo intercorso per il ritrovamento, nonostante la geolocalizzazione, lo *smartphone* era definitivamente uscito dalla sfera di controllo materiale del proprietario per entrare in modo pieno ed esclusivo in quella dell'autore del reato. Ancora, la giurisprudenza si è chiesta se potesse essere ritenuto sussistente lo stato di quasi flagranza nell'ipotesi in cui si fosse individuato il responsabile dell'autore del reato di furto grazie all'attività di tracciamento effettuata dalla persona offesa che aveva apposto sull'oggetto sottratto un *Air Tag*, vale a dire un dispositivo in grado di mapparne gli spostamenti. Nel senso della sussistenza della quasi flagranza si è espressa Cass. pen., sez. V, 19 dicembre 2023 n. 6421, E., in *CED Cass.*, n. 286085 – 01.

6. Controdeduzioni alla tesi dottrinale maggioritaria volta ad asserire la maggiore invasività della localizzazione satellitare rispetto al pedinamento

La dottrina, pressoché all'unisono, è solita affermare la maggiore invasività della localizzazione satellitare rispetto al pedinamento 'classico'[26].

A parere di chi scrive occorrerebbe invece rovesciare la prospettiva, dato che proprio il pedinamento appare l'indagine più invasiva. Per comprenderlo è però necessario uno sforzo ricostruttivo che non può prescindere dalla comprensione tecnica della localizzazione satellitare. Il che aiuterà a rifuggire da ogni approccio fideistico alla tecnologia, scoprendone la fallibilità, il suo margine di errore e i suoi limiti[27].

Consapevoli che la tesi della minore invasività della localizzazione satellitare rispetto al pedinamento si pone in linea di discontinuità con la dottrina del tutto maggioritaria, si analizzeranno in proseguo le ragioni che tale dottrina pone a fondamento della propria impostazione, offrendo delle controdeduzioni. Si verificherà dunque se la localizzazione satellitare si caratterizzi davvero per i seguenti profili: maggiore continuità della mappatura; più marcata incidenza sul piano della *privacy*; capacità di ricavare il 'profilo' dell'indagato sulla base del tracciamento; più elevato grado di precisione e certezza dei dati di localizzazione raccolti.

a. Iniziando dalla *continuità temporale*, il raffronto deve essere effettuato comparando le ipotesi in cui venga disposto un pedinamento e una localizzazione satellitare per il medesimo arco temporale, nei confronti del medesimo soggetto.

---

[26] Nel medesimo senso si è espresso anche il SENATO DELLA REPUBBLICA, *Documento approvato dalla 2ª Commissione permanente (Giustizia) nella seduta del 20 settembre 2023 a conclusione dell'indagine conoscitiva sul tema delle intercettazioni*, 2023, p. 38 ove in riferimento al «pedinamento elettronico, effettuato attraverso il captatore o il GPS» si precisa infatti che «rispetto al pedinamento 'ordinario' (eseguito dalla polizia giudiziaria) l'impiego della tecnologia determina un mutamento non solo quantitativo ma anche qualitativo che si manifesta nella pervasività del controllo».

[27] Si concorda dunque che la prova scientifica «deve essere calata nei consolidati canoni della epistemologia processuale». In questi termini, G. GARUTI, *Scienza e processo penale: introduzione al tema*, in *Archivio penale*, 2011, 3, p. 3.

Si è consapevoli che in dottrina si sostiene che, mentre il pedinamento 'classico' non potrebbe addentrarsi in certe zone, il c.d. pedinamento elettronico assicurerebbe invece un monitoraggio continuo.

Tale assunto sembra poter essere ripensato alla luce di due profili: uno tecnico e uno fattuale.

Quanto al limite tecnico, la localizzazione satellitare non è esente da soluzioni di continuità. In effetti, è sufficiente che il soggetto monitorato attraversi aree in cui il segnale di localizzazione non arrivi (si pensi a una galleria oppure a un'area schermata come quelle militari) o che si verifichino particolari situazioni climatiche (boschi con fronde bagnate dalla pioggia; forti nevicate; copertura nuvolosa densa; *etc.*) perché il tracciamento possa essere interrotto e ricominci solo successivamente, non appena il dispositivo sarà in grado di captare nuovamente il segnale.

Ne deriva che il reale funzionamento tecnico del localizzatore si pone in antitesi rispetto a quanto indicato dalla stessa Corte di Strasburgo, secondo la quale il localizzatore satellitare «permette la localizzazione continua, senza perdita di tempo, degli oggetti equipaggiati con un satellite GPS»[28].

Si potrebbe sostenere che è possibile individuare dei casi in cui la localizzazione satellitare riesca a giungere in luoghi preclusi all'ordinario pedinamento, come i luoghi di domicilio o i luoghi non visibili. Al riguardo, occorre anzitutto precisare che si tratterebbe di ipotesi del tutto residuali, anche perché non è detto che in simili luoghi arrivi il segnale satellitare (ad esempio, nel *garage* sotterraneo di un edificio in calcestruzzo armato di solito non è possibile alcuna localizzazione satellitare). Inoltre, va evidenziato che, di regola, lo stesso pedinamento 'classico' sarà in grado di individuare luoghi domiciliari, senza contare che la localizzazione satellitare fornisce solo la posizione di un veicolo e non anche quella del soggetto monitorato, che potrebbe invece essere percepita dal pedinamento 'classico', ad esempio perché l'indagato, dopo avere posto la macchina in *garage*, è riconoscibile all'interno del proprio salotto poiché le relative finestre sono visibili dalla strada pubblica.

[28] Cfr. Corte eur. dir. uomo, sez. V, sent. 2 settembre 2010, Uzun c. Germania, § 13.

Venendo all'aspetto fattuale, occorre rimarcare come il dispositivo volto alla localizzazione satellitare venga collocato sui veicoli e non sulle persone per l'evidente necessità che l'indagine resti occulta all'indagato. Tuttavia, ciò si riverbera nella circostanza che la localizzazione satellitare è in sé discontinua; infatti, diversamente dal pedinamento, essa non è in grado di monitorare gli spostamenti effettuati a piedi o con mezzi di locomozione diversi da quello in cui è installato il localizzatore satellitare, come dimostra il drammatico caso di Annalisa Baldovin, la cui uccisione avvenne da parte di un uomo, sulla cui vettura era stato installato nell'ambito delle indagini un localizzatore satellitare, ma che si avvalse di un *taxi* per raggiungerla e freddarla, sfuggendo così al monitoraggio.

b. Quanto alla incidenza sulla *privacy*, è proprio la localizzazione satellitare ad apparire meno invasiva rispetto al pedinamento 'classico', dato che soltanto quest'ultimo è in grado di apprendere una serie di informazioni.

Infatti solo il pedinamento tradizionale può osservare la persona cogliendone vari aspetti quali, a titolo meramente esemplificativo, problemi deambulatori resi evidenti dall'incedere della camminata; abbigliamento; persone che incontra; tratti prosodici; luoghi frequentati che possono fornire informazioni importanti su profili sanitari (come potrebbe accadere nel caso di ingresso in strutture dedicate in via esclusiva alla cura di determinate malattie), religiosi (che potrebbero essere desunti dal reiterato ingresso in luoghi deputati al culto o di estremismo religioso), orientamento sessuale (si pensi all'ingresso in locali frequentati soltanto da un determinato genere), *etc.*

Al contrario, la localizzazione satellitare è asettica, essendo in grado di individuare soltanto la latitudine, la longitudine e l'altitudine, nonché l'ora del rilevamento. In sintesi, essa fornisce il mero posizionamento in un determinato momento. Si noti, poi, che i dati di localizzazione riguardano il veicolo e non la persona monitorata, sicché residuerà il problema di verificare chi, in concreto, abbia utilizzato quel determinato mezzo di locomozione.

Tali considerazioni sospingono a ritenere che l'atto investigativo maggiormente invasivo della *privacy* consista nel pedinamento e non nella localizzazione satellitare.

c. Venendo alla possibilità di creare il 'profilo' dell'indagato, in dottrina si sostiene che i dati di localizzazione satellitare consentirebbero di essere combinati con altri dati, tracciando il profilo dell'indagato e divenendo uno strumento assai invasivo. Al riguardo, sembra possibile muovere tre rilievi.

Il primo è rappresentato dalla presa d'atto che, almeno di regola, l'attuale e assai scarna dotazione tecnologica[29] di procure e polizia giudiziaria non consente attività di creazione digitale di *criminal profiling*.

In ogni caso, quand'anche fosse possibile, allo stato della tecnica, una simile profilazione integrerebbe una attività successiva alla localizzazione. Sicché l'invasività andrebbe imputata a questa seconda attività di combinazione dei dati al fine della profilazione e non alla localizzazione satellitare in sé.

Infine, va rilevato un ulteriore aspetto. Anche il pedinamento può essere tradotto in dati, che potrebbero essere connessi con altri dati offrendo una profilazione. In particolare, se i dati del pedinamento tradizionale e di quello elettronico venissero combinati con i medesimi dati, tendenzialmente il *criminal profiling* più invasivo sarebbe quello derivante dal pedinamento tradizionale, per la ragione che solo quest'ultimo è in grado di fornire una serie di informazioni ulteriori rispetto a ora, latitudine, longitudine, altitudine, che sono invece appannaggio della localizzazione satellitare.

d. Infine, in riferimento alla asserita maggiore precisione e certezza dei dati di posizionamento ricavati mediante il dispositivo di localizzazione satellitare, occorre rifuggire da qualsiasi approccio fideistico alla tecnologia, ricordando invece come essa sia in sé fallibile[30].

---

[29] Il che rappresenta anche uno dei fattori ostativi alla piena attuazione del processo penale telematico, come ricordato da G. DI PAOLO, *Verso la modernizzazione del processo penale. Il contributo della 'riforma Cartabia' alla digitalizzazione del processo penale*, in *Alla ricerca di un processo penale efficiente. Atti del XXXV Convegno nazionale dell'Associazione tra gli studiosi del processo penale "G.D. Pisapia"*, Milano, 2024, p. 31.

[30] Per una più ampia riflessione sulla valenza accertativa delle indagini digitali, volta a porre in luce la necessità che, al tempo stesso, manchino fattori interferenti e che i dati raccolti siano correttamente interpretati si veda, volendo, S. SIGNORATO, *Indagini e prove digitali*, in *Riv. dir. process.*, 2024, p. 1166 ss.

Al riguardo, va precisato anzitutto come la localizzazione satellitare abbia un margine di errore di qualche metro, che può però aumentare a fronte di certe situazioni. Ad esempio, in zone su cui incombono monti, in determinati contesti, il margine di errore può raggiungere centinaia di metri. Più in generale, in tema di errore, rileva anche la distribuzione dei satelliti (di regola almeno quattro) da cui capta il segnale il localizzatore satellitare; infatti, da un punto di vista tecnico, più i satelliti sono vicini tra loro, più aumenta la c.d. diluizione geometrica di precisione (GDOP) con la conseguenza che aumenta anche il margine di errore.

Ne deriva che mentre un pedinamento 'classico' può apprendere che un determinato soggetto, a una certa ora, si è appoggiato con la mano destra allo stipite della porta di una determinata via e numero civico, la localizzazione satellitare potrà solo constatare, con un margine di errore più o meno marcato, che il veicolo monitorato si è fermato in un luogo.

Inoltre, la localizzazione satellitare si caratterizza per una idoneità accertativa solo nel caso in cui sia possibile escludere l'impiego di *jammer* o di tecniche di *spoofing*.

Il *jammer* è un dispositivo che consente di schermare il segnale. Di conseguenza, il suo utilizzo funge da mezzo per sfuggire alle indagini. Nello specifico, se in un veicolo in cui è stato installato un localizzatore satellitare a fini di indagine penale venisse attivato un *jammer*, quest'ultimo schermerebbe il segnale satellitare, sicché la polizia giudiziaria visualizzerebbe quel veicolo come fermo nonostante si stia in realtà spostando.

Diverso dal *jammer* è lo *spoofing*. Mentre il primo scherma il segnale, il secondo lo altera, con la conseguenza che l'impiego dello *spoofing* fa sì che gli investigatori ricevano dati di localizzazione differenti dal reale.

Ne deriva che un pedinamento 'classico' svolto con professionalità può risultare più preciso della localizzazione satellitare non essendo soggetto al margine di errore tecnico e alla possibilità di vedere alterati i dati.

In conclusione, l'analisi dei profili della continuità temporale, della violazione della *privacy*, della profilazione e della correttezza dei dati raccolti porta a ritenere che, rispetto alla localizzazione satellitare, il

pedinamento 'classico' sia una tipologia investigativa più invasiva in termini di rispetto dei diritti dell'indagato.

Tutt'altro discorso, invece, è la circostanza che un ordinario pedinamento sia una attività che implica dei rischi per il personale della polizia giudiziaria; inoltre, non potendo essere effettuato sempre dalle stesse persone, esso comporta un significativo impiego di uomini. Sotto il profilo del rischio e dei costi, per la polizia giudiziaria il pedinamento può risultare più gravoso della localizzazione satellitare. Tuttavia, se il punto di osservazione resta quello del rispetto dei diritti fondamentali dell'indagato, è proprio il pedinamento a essere più invasivo della localizzazione satellitare.

7. Rifluenze dell'inquadramento giuridico della geolocalizzazione sulle attività captative oltre confine

La qualificazione giuridica della localizzazione satellitare in termini di pedinamento elettronico pare esplicare significativi riverberi anche sul piano dell'acquisizione all'estero dei dati di localizzazione.

Per comprendere appieno la problematica sembra opportuno muovere da lontano ricordando i conflitti che dilaniarono una parte dell'Europa tra il 1618 e il 1648 (c.d. Guerra dei Trent'Anni). A essi seguì la Pace di Vestfalia, la quale affermò il concetto di confine sancendo che ogni Stato è sovrano solo entro tale limite.

Sul piano investigativo, salve alcune particolari ipotesi[31], ciò implica che l'acquisizione della prova all'estero è legittima solo attivando i meccanismi di cooperazione. Un simile approccio non è però scevro di

[31] A titolo esemplificativo cfr. Regolamento (UE) 2021/784, che consente agli Stati membri di emettere ordini di rimozione di contenuti terroristici *on line* o di disabilitazione dell'accesso a tali contenuti, rivolgendo tali ordini direttamente ai prestatori di servizi di *hosting*, a prescindere dallo Stato a cui questi ultimi afferiscono. Al riguardo, volendo S. SIGNORATO, *Combating terrorism on the internet to protect the right to life. The regulation (EU) 2021/784 on addressing the dissemination of terrorist content online*, in *Provincial Protector of Citizens*, Ombudsman (Ed.), *Yearbook. Human rights protection. The right to life, Vojvodina Provincial authorities Common Affairs Department Novi Sad, Republic of Serbia*, 2021, pp. 403-408.

farraginosità, senza contare la sua negativa incidenza sulle tempistiche di acquisizione della prova all'estero. Per questo motivo, si registrano spinte eccentriche. Tra esse si può ricordare l'art. 32 della Convenzione di Budapest[32], attuato con l'art. 234-*bis* c.p.p., il quale prevede tra l'altro la possibilità di acquisizione diretta (quindi, senza l'attivazione di forme di cooperazione) di documenti e dati informatici conservati all'estero che siano disponibili al pubblico (si pensi a una foto reperibile su *Google* immagini)[33].

Fatta questa premessa, occorre precisare come la tecnologia abbia schiuso inedite possibilità, rendendo possibile la trasmissione di elementi di prova anche in maniera virtuale[34].

Quid iuris, dunque, se il veicolo su cui è stato installato un localizzatore satellitare attraversa i confini nazionali, continuando a trasmettere le informazioni di posizionamento agli investigatori situati in Italia? Se la regola è la necessità di attivare la cooperazione investigativa ogni volta che si valichi il confine nazionale, si deve ritenere che sia necessario il ricorso a essa anche in una simile ipotesi?

Dal canto suo, la giurisprudenza tende a fare leva sul consolidato concetto di instradamento, vale a dire sull'impiego di strumentazione interamente italiana, senza che sia necessaria l'assistenza di alcun altro Stato. Non solo in materia di intercettazioni ma anche di localizzazione satellitare si afferma conseguentemente che, se il dispositivo di monitoraggio «viene collocato nel territorio dello Stato su veicolo o altra cosa che poi successivamente si sposta all'estero, l'utilizzazione dei risultati del tracciamento degli spostamenti avvenuti all'estero non necessiti di

[32] Si tratta della Convenzione del Consiglio d'Europa sulla criminalità informatica aperta alla firma a Budapest il 23 novembre 2001, resa esecutiva con l. 18 marzo 2008 n. 48 ed entrata in vigore per l'Italia il 1º ottobre 2008.

[33] Occorre precisare come l'art. 234-*bis* c.p.p. escluda la cooperazione investigativa pure in una seconda ipotesi rappresentata dal consenso del legittimo titolare all'acquisizione di documenti e dati informatici siti all'estero e diversi da quelli disponibili al pubblico.

[34] Si veda F. SIRACUSANO, *La prova informatica transnazionale: un difficile 'connubio' fra innovazione e tradizione*, in *Processo penale e giustizia*, 2017, 1, p. 181, che, in rapporto alle prove elettroniche, pone in luce la loro «sostanziale 'incapacità' a essere ricondotte entro i tradizionali confini della cooperazione giudiziaria».

rogatoria internazionale»[35], né, ove applicabile, dell'ordine europeo di indagine penale (c.d. OEI)[36].

Tuttavia, in materia di intercettazioni, una simile impostazione deve ora coniugarsi con l'art. 31 direttiva OEI[37], il quale prevede l'obbligo di notifica allo Stato membro ove si trova la persona intercettata, anche nel caso in cui non sia necessaria l'assistenza tecnica di tale Stato. Si noti che a quest'ultimo Stato viene espressamente riconosciuto il potere di disporre che l'intercettazione non venga effettuata o che sia interrotta o che non siano utilizzabili gli esiti se una simile intercettazione non sarebbe ammessa in un caso interno analogo.

Il fatto di ritenere che la geolocalizzazione non integri una forma di intercettazione ha una importante ricaduta giuridica perché sottrae tale indagine al perimetro di applicabilità dell'art. 31 direttiva OEI. È dunque possibile individuare un primo punto fermo: la localizzazione satellitare che prosegua all'estero sembra sfuggire alla necessità di notifica *ex* art. 31 direttiva OEI.

*8. Segue: l'applicabilità dell'art. 234-*bis *c.p.p. e dell'art. 40 CAAS alla localizzazione satellitare all'estero*

Si tratta di comprendere se l'attività di monitoraggio satellitare all'estero postuli il ricorso agli ordinari strumenti della cooperazione investigativa. Nel par. 4 si è precisato come la localizzazione satellitare non integri una forma di intercettazione non solo perché non capta alcun contenuto comunicativo, ma anche perché apprende un segnale che non è riservato ma disponibile a chiunque. Tale aspetto tecnologico appare dirimente per ritenere applicabile alla localizzazione satellitare oltre confine l'art. 32 della Convenzione di Budapest e l'art. 234-*bis*

[35] In questi termini, si veda Cass. pen., sez. I, sent. 1º marzo 2023, n. 20859.

[36] Per un approfondimento degli strumenti di cooperazione, cfr. M. DANIELE (aggiornamento di S. Signorato), *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, in A. CADOPPI et al., *Cybercrime*, II ed., Torino, 2023, p. 1892 ss.

[37] Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale.

c.p.p., i quali consentono l'acquisizione diretta dei dati disponibili al pubblico, senza che ricorra alcuna necessità di attivare gli strumenti della cooperazione investigativa[38].

Contro una simile impostazione, potrebbero forse essere poste due obiezioni.

La prima potrebbe fare leva sul caso *Sky Ecc* rispetto al quale la riflessione dottrinale e giurisprudenziale aveva precisato come l'art. 234-*bis* c.p.p. si applicasse nel caso di prove preesistenti ed esterne all'attività investigativa. Tale tesi, sostenuta dalle sezioni unite della Cassazione[39] e da parte della dottrina, deve essere compresa per ciò che essa dice, in quanto sia la dottrina che la giurisprudenza stavano ragionando di un caso in cui si era trattato di acquisire documenti, ancorché informatici. Dunque, le caratteristiche della preesistenza e della estraneità all'attività investigativa derivavano non dalla disciplina dell'art. 234-*bis* c.p.p., ma dal documento che, in quanto tale, è prova precostituita e non può essere formato in sede investigativa, configurando quest'ultima ipotesi una attività di documentazione, secondo una differenziazione che è il «naturale portato del principio di separazione tra fasi»[40].

Di conseguenza, la disciplina prevista dall'art. 234-*bis* c.p.p. volta alla acquisizione di dati informatici si può applicare anche a dati acquisiti sincronicamente e nell'ambito di una attività investigativa. In ogni caso, a voler essere microchirurgici, il dato del segnale satellitare preesiste alla sua captazione per fini di localizzazione.

La seconda critica che potrebbe essere mossa alla tesi sostenuta dalla scrivente (il fatto che la disciplina prevista dall'art. 234-*bis* c.p.p. si applichi anche nei casi di acquisizione investigativa sincrona di dati informatici) potrebbe forse focalizzarsi sul dato testuale, sostenendo che

[38] Come condivisibilmente chiarito da Cass., sez. un., sent. 29 febbraio 2024 n. 23755, G., § 6, in *CED Cass.*, n. 286573, nonché da Cass., sez. un., sent. 29 febbraio 2024 n. 23756, G., § 9, in *CED Cass.*, n. 286589, l'art. 234-*bis* legittima una tipologia investigativa «alternativa e incompatibile rispetto a quella dettata in tema di ordine europeo di indagine». Sul tema, in dottrina, cfr. M. DANIELE, *La mappa del controllo giurisdizionale quando l'OEI ha ad oggetto prove già in possesso dell'autorità straniera*, in *Sistema penale* (rivista web), 17 luglio 2024 (ultimo accesso il 28 febbraio 2025).

[39] Cfr. Cass., sez. un., sent. 29 febbraio 2024 n. 23755 e n. 23756.

[40] In questi termini, C. cost., sent. 30 novembre 2011 n. 320, § 7 del *Considerato in diritto*.

l'art. 234-*bis* c.p.p. si riferisce ai dati informatici, mentre i segnali emessi dal satellite sono elettrici. Se formulata, una simile obiezione non coglierebbe nel segno. Infatti, se l'art. 234 *bis* c.p.p. consente l'acquisizione di dati informatici, a maggior ragione esso deve permettere la captazione dei segnali elettrici che si caratterizzano per una minore invasività. Inoltre, dopo la captazione del segnale, si generano dati informatici che consentono agli investigatori di conoscere la localizzazione.

In sintesi, a parere di chi scrive, la localizzazione satellitare che prosegua oltre confine integra una attività investigativa che non richiede l'attivazione di alcuno strumento di cooperazione tra Stati, essendo legittima in forza dell'art. 234-*bis* c.p.p. Ne consegue la piena utilizzabilità processuale dei dati di localizzazione raccolti.

Si può ricordare che, qualora non si ritenesse di accedere a questa impostazione, dalla qualificazione della localizzazione satellitare in termini di pedinamento elettronico discenderebbe anche l'applicabilità di una ulteriore previsione, almeno entro il perimetro applicativo della Convenzione di applicazione dell'accordo di Schengen (CAAS).

Il riferimento è all'art. 40 CAAS il quale disciplina l'osservazione transfrontaliera. In una simile ipotesi, però, la prosecuzione della localizzazione satellitare sarebbe subordinata a una serie di requisiti. Anzitutto, il monitoraggio dovrebbe riguardare un soggetto che «si presume abbia partecipato alla commissione di un reato che può dar luogo a estradizione». In secondo luogo, dovrebbe sussistere l'autorizzazione da parte dello Stato ove si trova l'indagato, che sia stata rilasciata in forza di una domanda di assistenza giudiziaria preventivamente presentata. Fanno eccezione soltanto i casi di particolare urgenza, ma il passaggio della frontiera andrebbe immediatamente comunicato e dovrebbe essere trasmessa «senza indugio» la richiesta di assistenza giudiziaria. Infine, resta ferma la possibilità che lo Stato richiesto stabilisca l'interruzione della osservazione o subordini l'autorizzazione a determinate condizioni.

9. I diritti in gioco nella localizzazione satellitare e nel pedinamento 'classico'

Sembra opportuno chiedersi su quali sfere di tutela incidano la localizzazione satellitare e il pedinamento 'classico' per verificare se il loro svolgimento sia assistito da idonee garanzie.

Al riguardo si può precisare anzitutto come la localizzazione satellitare non determini alcuna compressione del diritto alla libertà e alla segretezza della corrispondenza e di ogni altra forma di comunicazione, dato che non viene captata alcuna comunicazione.

Invece, non è escluso che, occasionalmente, il pedinamento possa apprendere comunicazioni[41], sicché si potrebbe porre un problema di ingerenza nell'art. 15 Cost., con conseguente necessità di atto motivato dell'autorità giudiziaria[42]. Il che è stato peraltro totalmente disatteso nella prassi operativa, dove è sedimentato il ricorso al pedinamento come mera attività di polizia giudiziaria o attività autorizzata/delegata dal pubblico ministero, senza che vi sia a monte alcun decreto motivato del giudice per le indagini preliminari.

Si può poi evidenziare come né la localizzazione satellitare né il pedinamento 'classico' determinino alcuna ingerenza nella garanzia *ex* art. 13 Cost. Invero, in quanto occulte, non incidono sulla libertà personale[43], nonostante si sia assistito a una dilatazione di tale sfera di tutela.

---

[41] Sul tema dell'ascolto casuale del colloquio, per tutti, si rinvia a F. CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2000, p. 160 ss.

[42] Sull'ipotesi della registrazione eseguita dalla polizia giudiziaria nel corso di un pedinamento, cfr., *ex multis*, K. LA REGINA, *L'identificazione della voce nel processo penale*, Padova, 2018, p. 17.

[43] In senso contrario, si veda L. FILIPPI, *Il GPS è una prova 'incostituzionale'? Domanda provocatoria, ma non troppo, dopo la sentenza Jones della Corte Suprema U.S.A.*, in *Archivio penale*, 2012, 1, p. 7. In argomento, cfr. anche *Supreme Court of the United States, U.S. v. Jones*, 23 gennaio 2012, la quale, riconoscendo che l'installazione del localizzatore satellitare aveva determinato un *trespassing*, ha ritenuto sussistente la violazione del IV emendamento. Per un approfondimento sul tema v. anche G. DI PAOLO, *Acquisizione dinamica dei dati relativi all'ubicazione del cellulare e altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense*, cit., p. 223 ss.; nonché F. IOVENE, *Pedinamento satellitare e diritti fondamentali della persona*, in *Cass. pen.*, 2012, p. 3559 ss. e C. CONTI, *Annullamento per violazione*

Una parte della dottrina ha invece evidenziato la possibile limitazione della libertà prevista dall'art. 16 Cost. sul presupposto che una lettura della previsione costituzionale che tenga conto dell'evoluzione tecnologica della società consentirebbe di individuare una nuova declinazione della libertà di circolare, rappresentata dal «diritto a non essere localizzati»[44].

Infine, se il pedinamento di regola non incide sull'inviolabilità del domicilio, nel caso della localizzazione satellitare si potrebbero individuare sparuti casi di compressione dell'art. 14 Cost. qualora si consideri l'interno di un veicolo (si pensi in particolare a un *camper*) alla stregua di un domicilio[45] e ivi venga posizionato il localizzatore satellitare[46]. In simili ipotesi, *ex* art. 14 Cost., tale localizzatore potrebbe essere posizionato solo in forza di un atto motivato dell'autorità giudiziaria. Di regola, però, non vi è alcuna incidenza sull'inviolabilità del domicilio, dato che il localizzatore satellitare viene ubicato sul vano motore o in zone esterne all'abitacolo.

---

di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali, in *Cass. pen.*, 2013, 10, p. 492.

[44] Così A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005, 2, p. 632 s. Cfr., inoltre, G. DI PAOLO, *Acquisizione dinamica dei dati relativi all'ubicazione del cellulare e altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense*, cit., p. 238.

[45] Al di là dei veicoli che fungono anche da abitazione, appare rara la qualificazione in termini di domicilio dell'abitacolo di una vettura. In tal senso si vedano però C. cost., sent. 25 marzo 1987 n. 88; Cass. pen., sez. II, sent. 10 giugno 1998, Z., in *Cass. pen.*, 2000, p. 2026.

[46] L'installazione del dispositivo è una attività prodromica alla localizzazione satellitare. Per una riflessione sistemica sul tema di tali attività, anche in rapporto alla distinzione di fondo contenitore-contenuto, si rinvia a L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali*, in *Diritti della persona e nuove sfide del processo penale. Atti del XXXII Convegno nazionale dell'Associazione tra gli studiosi del processo penale "G.D. Pisapia"*, Milano, 2019, p. 217.

10. Segue: riflessioni in tema di diritto al rispetto della vita privata e familiare ex *art. 8 Cedu*

Il pedinamento e la localizzazione satellitare incidono invece sulla *privacy*. In questo senso si è espressa anche la Corte di Strasburgo, che si è trovata a riflettere sulla localizzazione satellitare.

In particolare, nel caso Uzun contro Germania, la Corte eur. dir. uomo ha affermato che la localizzazione satellitare interferisce sul diritto al rispetto della vita privata e familiare[47], precisando peraltro che tale *vulnus* avviene in misura minore rispetto «agli altri metodi di sorveglianza visiva o acustica»[48].

La minore invasività della localizzazione satellitare rispetto alle altre tecniche di sorveglianza è stata successivamente rimarcata dalla medesima Corte anche nel caso Ben Faiza contro Francia[49], sul presupposto che la localizzazione satellitare non è in grado di fornire informazioni circa la condotta, le opinioni o i sentimenti degli indagati che possono invece essere captati da altri mezzi di sorveglianza[50].

Ciò premesso resta il problema di verificare se la disciplina interna sia o non sia compatibile con l'art. 8 Cedu che tutela il diritto al rispetto della vita privata e familiare, ricomprendendo in esso anche la tutela del domicilio. Le criticità si addensano sul fatto che dall'art. 8 Cedu, così come interpretato dalla Corte di Strasburgo, deriva che un'attività investigativa che viola la *privacy* è legittima solo se soddisfa i seguenti tre requisiti.

Anzitutto, deve rappresentare una misura che in una società democratica sia finalizzata a preservare tutele ulteriori, tra le quali figurano

---

[47] Sul fatto che il diritto al rispetto della vita privata e familiare si declinerebbe anche nei luoghi pubblici o aperti al pubblico, cfr. C. FANUELE, *Il rilevamento satellitare tramite GPS: una prassi da ancorare ai principi stabiliti dalla Cedu*, in *Dir. pen. proc.*, 2019, 12, p. 1707.

[48] Cfr. Corte eur. dir. uomo, sez V., sent. 2 settembre 2010, Uzun c. Germania, § 49.

[49] Si veda Corte eur. dir. uomo, sez. V, sent. 8 febbraio 2018, Ben Faiza c. Francia, § 53.

[50] Come chiarito da D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 2020, 1, p. 17, la localizzazione satellitare «non tocca il nucleo incomprimibile della vita privata».

la sicurezza nazionale, la pubblica sicurezza, il benessere economico del paese, la difesa dell'ordine, la prevenzione dei reati, la protezione dei diritti e delle libertà altrui. Essendo finalizzati alla prevenzione o repressione dei reati, il pedinamento e la localizzazione satellitare appaiono soddisfare appieno il requisito in esame richiesto dall'art. 8 Cedu.

In secondo luogo, l'ingerenza deve essere proporzionata[51] alla finalità da raggiungere. Si tratta di un aspetto che andrà soppesato in concreto, anche se, in ragione della scarsa incidenza sulla *privacy* quantomeno da parte della localizzazione satellitare, è da ritenere che almeno quest'ultima sia di regola proporzionata.

Più critico l'ulteriore requisito previsto dall'art. 8 Cedu, il quale ritiene legittima l'ingerenza nella *privacy* solo in presenza di una «previsione di legge», la quale, oltretutto, secondo la giurisprudenza della Corte europea, deve essere assistita da idonee garanzie. Questo requisito si pone in rapporto di frizione con la disciplina interna che ammette la possibilità di svolgere atti investigativi atipici, in quanto tali non previsti dalla legge.

L'approccio del legislatore italiano può apparire convincente perché occorre rifuggire da una eccessiva ingessatura e dall'incasellamento della fase delle indagini, la quale, per sua natura, richiede duttilità. Al tempo stesso, però, laddove vi sia una marcata ingerenza nei diritti fondamentali, gli atti investigativi non possono essere lasciati nell'alveo della atipicità, come accade attualmente per il *trojan*, che il legislatore italiano ha disciplinato soltanto in rapporto all'inoculazione nei dispositivi mobili e nella sua mera funzione intercettativa, oltretutto tra presen-

[51] Per un approfondimento sul principio di proporzionalità, si rinvia A. STONE SWEET, J. MATHEWS, *Proportionality Balancing and Global Constitutionalism*, in *Columbia Journal of Transnational Law* 47, 1, 2008, pp. 73-164; G. LÜBBE-WOLFF, *The Principle of Proportionality in the Case-Law of the German Federal Constitutional Court*, in *Human Rights Law Journal*, 2014, p. 12 ss.; M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Diritto penale contemporaneo - Rivista trimestrale*, 2014, 3-4, p. 143; D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 2020, 1, p. 3 ss.; R. APRATI, *Prime riflessioni sull'assetto normativo del captatore informatico*, in *Cass. pen.*, 2021, 2, p. 453; R. ORLANDI, *Uso poliziesco dell'intelligenza artificiale. L'insegnamento del* Bundesverfassungsgericht, in *Cass. pen.*, 2023, 7/8, p. 2171 ss.

ti, relegando *sub* art. 189 c.p.p. tutti i restanti usi del captatore informatico.

Venendo a pedinamento e localizzazione satellitare, per capire se essi siano in linea con l'art. 8 Cedu, occorre anzitutto verificare la previsione di legge che li sorregge, la quale, come si diceva, può essere individuata negli artt. 55, 348, 189 c.p.p., anche se non di rado vengono effettuati come attività delegata *ex* art. 370 c.p.p. Se, dunque, sussistono delle previsioni di legge, residuano dei dubbi circa l'art. 189 c.p.p. dato che ci si potrebbe chiedere se una norma rubricata *Prove non disciplinate dalla legge* funga da ossimoro rispetto al requisito della previsione di legge o sia comunque sufficiente a integrare tale requisito[52]. I nodi problematici si acuiscono, però, in rapporto alla verifica del requisito richiesto dalla Cedu circa le idonee garanzie che devono assistere la previsione di legge volta a legittimare l'ingerenza nella *privacy*.

Se l'attività di pedinamento o di localizzazione satellitare viene svolta come attività delegata *ex* art. 370 c.p.p. la garanzia appare in effetti sufficiente, dato che c'è a monte un vaglio dell'autorità giudiziaria.

Più difficile capire se le tutele possano ritenersi in effetti adeguate qualora l'inquadramento giuridico ricada *sub* art. 55 o 348 c.p.p. confluendo peraltro nell'art. 189 c.p.p. La criticità si incunea nel fatto che, come si è ricordato, l'art. 8 Cedu, così come interpretato dalla Corte di Strasburgo, richiede l'esistenza di idonee garanzie, mentre le summenzionate previsioni sono assistite da tutele blande, rappresentate dalla idoneità della tecnica investigativa all'accertamento del fatto, dal non pregiudizio sulla libertà morale e dall'espletamento di un contraddittorio che, come indicato in dottrina, nel caso degli atti occulti, potrebbe svolgersi postumo[53]. Nemmeno la Costituzione offre un baluardo garantista, se è vero che la tutela della *privacy* sembra ricadere sotto l'om-

[52] Sotto altro profilo, reputa che l'art. 189 c.p.p. sia inidoneo a integrare il requisito della riserva di legge prevista dalla Costituzione, T. BENE, *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2019, p. 456.

[53] Sul tema, si rinvia ad A. CAMON, *Le sezioni unite sulle videoregistrazioni come prova penale: qualche chiarimento e alcuni dubbi nuovi*, in *Riv. dir. process.*, 2006, p. 1550 ss.

brello dell'art. 2 Cost., il quale, come noto, non postula il rispetto di alcuna garanzia.

Considerato che le norme della Cedu, nell'applicazione datane dalla Corte di Strasburgo, costituiscono parametro interposto di costituzionalità della normativa interna, non è da escludere che qualcuno possa sollevare questione di legittimità costituzionale, in rapporto all'art. 117, co. 1 Cost. e 8 Cedu, degli artt. 55, 348, 189 c.p.p. nella parte in cui essi non prevedono alcuna garanzia o non prevedono garanzie sufficienti.

Allo stato, è difficile pronosticare quale potrebbe essere la decisione in un eventuale giudizio instaurato innanzi alla Corte di Strasburgo e, in particolare, se la disciplina italiana del pedinamento e della localizzazione satellitare verrà o non verrà ritenuta soddisfacente rispetto al requisito *ex* art. 8 Cedu della previsione di legge assistita da idonee garanzie.

11. I dati di localizzazione dei tabulati

Se, per quanto riguarda il pedinamento 'classico' e la localizzazione satellitare, si versa in ipotesi di atipicità[54], ben più pregnanti sono le tutele allorché i dati di localizzazione siano dati esterni alle comunicazioni. In una simile ipotesi vi è infatti una norma *ad hoc*, assistita oltretutto da garanzie particolarmente marcate.

Il riferimento è all'art. 132 d.lgs. 30 giugno 2003, n. 196, il quale rappresenta una norma processuale penale innestata nel codice *privacy*. Tale previsione si caratterizza per una storia particolarmente travagliata, in cui si rincorrono continui ritocchi e modifiche della disciplina, che non di rado riflettono spinte e controspinte sovranazionali.

Basti pensare che la norma appariva in linea con quanto previsto dalla direttiva 2006/24/CE (c.d. direttiva Frattini), ma la stessa direttiva

[54] Rileva come in materia di localizzazione satellitare non esista un 'diritto di natura', residuando dunque la possibilità che ordinamenti diversi disciplinino in modo differente tale mezzo di ricerca della prova, C. CONTI, *Il principio di non sostituibilità: il sistema probatorio tra Costituzione e legge ordinaria*, in *Cass. pen.*, 2024, 2, p. 459.

è stata poi dichiarata invalida dalla Corte di giustizia[55], sul presupposto che tale atto non era rispettoso del principio di proporzionalità, con conseguente riviviscenza della direttiva 2022/58/CE, il cui art. 2, co. 1 lett. c) stabilisce che per «dati relativi all'ubicazione» si intende «ogni dato trattato in una rete di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico».

Occorre anzitutto chiarire che cosa preveda la disciplina *ex* art. 132 codice *privacy*. Per comprenderlo è opportuno ricordare che i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione dispongono di dati che possono essere fondamentali a fini investigativi e accertativi. Per questo motivo gli Stati impongono a tali fornitori, per determinati archi temporali, degli obblighi di legge di conservazione dei dati di traffico telefonico, telematico e relativi alle chiamate senza risposta. Tale disciplina viene di regola denominata *data retention*.

In particolare, tra i dati che si chiede loro di conservare rientrano, a titolo esemplificativo, i dati che permettono di rintracciare e identificare la fonte[56] e la destinazione[57] di una comunicazione; i dati funzionali a

[55] Cfr. CGUE, grande sezione, sent. 8 aprile 2014, cause C-293/12 e C-594/12, *Digital Right Ireland Ltdc. Minister for Communications, Marine and Natural Resources*. In tema si rinvia a R. FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. 'data retention' contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Diritto penale contemporaneo - Rivista trimestrale*, 2014, 2, p. 178 ss., nonché F. RUGGIERI, Data retention *e giudice di merito penale. Una discutibile pronuncia*, in *Cass. pen.*, 2017, p. 2483 ss.

[56] Al riguardo, per la telefonia di rete fissa e la telefonia mobile tra i dati conservati si possono ricordare il nome e l'indirizzo dell'abbonato o dell'utente registrato, nonché il numero telefonico del chiamante; quanto ai servizi telematici, vengono invece conservati i dati identificativi dell'utente; l'identificativo dell'utente e il numero telefonico assegnati a ogni comunicazione sulla rete telefonica pubblica; il nome e l'indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati assegnati l'indirizzo di protocollo Internet (IP), un identificativo di utente o un numero telefonico.

[57] Tra essi possono essere annoverati, per la telefonia di rete fissa e la telefonia mobile, il numero o i numeri chiamati, il numero a cui è stata inviata la chiamata nel caso di inoltro o trasferimento di chiamata, il nome e l'indirizzo dell'abbonato o dell'utente registrato; quanto alla posta elettronica su Internet e alla telefonia via Internet, viene in-

individuare la data, l'ora e la durata di una comunicazione; i dati che permettono di determinare il tipo di comunicazione; i dati che servono a identificare le attrezzature di comunicazione utilizzate dagli utenti o quelle che si presumono essere le loro attrezzature; i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile[58].

Proprio quest'ultima tipologia di dati appare di particolare interesse perché permette di individuare la posizione, esattamente come accade con la localizzazione satellitare. Sul piano delle tutele, però, le garanzie sono ben diverse.

Infatti, mentre il pedinamento 'classico' e la localizzazione satellitare di regola non abbisognano di alcun decreto dell'autorità giudiziaria[59], nel caso di raccolta di dati di localizzazione esterni alle comunicazioni e acquisiti in forza dell'art. 132 codice *privacy* si richiede invece un decreto motivato del giudice su richiesta del pubblico ministero o su istanza del difensore dell'imputato, dell'indagato, della persona offesa e delle altre parti private. Tale garanzia rafforzata è stata introdotta a seguito di una sentenza della Corte di giustizia dell'Unione europea[60] riguardante un caso estone, in cui la Corte di Lussemburgo aveva fatto leva sull'art. 15 § 1 della direttiva 2002/58/CE sancendo come esso osti a una normativa nazionale che permetta al pubblico ministero di autoriz-

---

vece conservato l'identificativo dell'utente o il numero telefonico del presunto destinatario della chiamata telefonica via Internet; il nome e l'indirizzo dell'abbonato o dell'utente registrato e l'identificativo del presunto destinatario della comunicazione.

[58] Premesso che la localizzazione può avvenire anche sulla base dell'indirizzo IP, appare interessante come si faccia riferimento a tale dato di traffico telematico anche in altri settori. Ne è una riprova il Testo unico dei tributi erariali minori (d.lgs. 5 novembre 2024, n. 174) il cui art. 72 (Localizzazione del dispositivo) ha espressamente previsto che un dispositivo si considera ubicato nel territorio dello Stato facendo «principalmente riferimento all'indirizzo di protocollo Internet (IP) del dispositivo stesso o ad altro sistema di geolocalizzazione, nel rispetto delle regole relative al trattamento dei dati personali».

[59] In senso conforme, con precipuo riferimento alla localizzazione satellitare, cfr. Cass. pen., sez. II, sent. 18 settembre 2024 n. 37395, B., in *CED Cass.*, n. 286949.

[60] Si tratta di CGUE, grande camera, sent. 2 marzo 2021, causa C-746/18, H.K. c. Prokuratuur. Al riguardo, cfr. E. ANDOLINA, *La sentenza della Corte di giustizia UE nel caso H.K. c. Prokuratuur: un punto di non ritorno nella lunga querelle in materia di* data retention*?*, in *Dir. pen. proc.*, 2021, 5, p. 1195 ss.

zare direttamente l'acquisizione di tali dati, in assenza di un controllo da parte di un giudice ovvero di «un'entità amministrativa indipendente».

Tale approdo è in linea con la dottrina del tutto maggioritaria[61] che individua nella conservazione dei dati di traffico telefonico, telematico, delle chiamate senza risposta una profonda incidenza sul piano dei diritti fondamentali, secondo una impostazione accolta anche dalla Corte di giustizia[62].

Dal canto suo, poi, la Corte costituzionale ha rimarcato «come non possa ravvisarsi una differenza ontologica tra il contenuto di una conversazione o di una comunicazione e il documento che rivela i dati estrinseci di queste»[63], assimilando la *data retention* alle intercettazioni.

In senso contrario, in dottrina è stato evidenziato come «quanto all'oggetto delle operazioni intercettive, va immediatamente precisato che può essere tale soltanto il *contenuto* delle comunicazioni», con esclusione delle

> «attività istruttorie finalizzate all'accertamento dei 'dati esteriori' della comunicazione (identità del mittente e del destinatario, forma dell'atto comunicativo, collocazione spazio-temporale, ecc.). In particolare, non è sostenibile che siano regolati dagli artt. 266-271 c.p.p. e 89

[61] Per l'impostazione secondo la quale l'autorizzazione del Giudice se non a livello costituzionale, ma almeno sul piano dell'opportunità andrebbe accolta con favore, si rinvia ad A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc.*, 2005, 2, p. 603, il quale afferma: «la scelta va senz'altro approvata, per tre motivi. Anzitutto, un organo in posizione d'equidistanza è ovviamente più adatto a effettuare un bilanciamento fra le ragioni dell'investigazione e quelle della libertà individuale. In secondo luogo, concentrare l'incombenza nelle mani del pubblico ministero avrebbe finito per manomettere le prospettive d'indagine del difensore, che, per acquisire determinate informazioni, avrebbe dovuto sollecitare l'antagonista. Infine, come sarà osservato in seguito, in omaggio all'idea del 'doppio binario' le nuove norme dettano, almeno in certe situazioni, regole diverse a seconda del reato su cui vertono le indagini; e "se il procedimento penale si articola in regimi diversificati a seconda della gravità dei reati", "è elementare regola di legalità che la scelta che condiziona il regime sia sottoposta a un controllo" del giudice».

[62] Al riguardo, si veda CGUE, grande camera, sent. 30 aprile 2024, causa C-178/22, Ignoti con l'intervento di Procura della Repubblica presso il Tribunale di Bolzano.

[63] Cfr. C. cost., sent. 27 luglio 2023 n. 170, § 4.4 del *Considerato in Diritto*.

disp. att. c.p.p. gli atti di acquisizione dei tabulati delle aziende telefoniche»[64].

Tale tesi appare del tutto convincente.

Infatti, in forza della disciplina *ex* art. 132 codice *privacy* non può mai essere acquisito il contenuto comunicativo. Non per nulla tali dati vengono denominati dati «esterni» alle comunicazioni. Se questo è vero, sul piano dei diritti fondamentali ben diversa è l'ingerenza della captazione di contenuto comunicativo o della raccolta di dati in grado di indicare soltanto l'ora o i luoghi in cui si è spostato il cellulare. Si noti, poi, che una simile localizzazione non fornisce l'esatta posizione dell'indagato, ma solo quella della cella a cui si aggancia il cellulare (per far comprendere la problematica, può essere ricordato come, talora, basti cambiare stanza all'interno della medesima abitazione perché il telefono cellulare si agganci a celle telefoniche diverse).

Se la scelta di richiedere un decreto del giudice per le indagini preliminari è comprensibile in un'ottica di medicina preventiva volta a scongiurare il rischio di condanne all'Italia, non sfugge come essa possa tradursi in una garanzia meramente formale. Invero, una tutela è tale quando è effettiva. Al riguardo, occorrerebbe comprendere se i giudici percepiscano tale vaglio alla stregua di una preziosa garanzia o quale mero aggravio ed ulteriore adempimento pressoché burocratico. In assenza di dati al riguardo, si può solo rilevare come, da una ricerca condotta sul piano nazionale, sia emerso che i casi di diniego da parte del giudice per le indagini preliminari all'acquisizione dei dati di traffico telefonico e telematico rappresentino una evenienza davvero rara[65]. L'assetto autorizzativo ha però comportato un ulteriore aggravio per gli uffici g.i.p. e, talora, un rallentamento delle indagini, dato che non sempre l'autorizzazione del giudice si colloca temporalmente nell'immediatezza della richiesta del pubblico ministero, determinando talora un pregiudizio per le indagini.

---

[64] Così, testualmente, F. CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2000, pp. 165-166.

[65] Tendenzialmente circoscritta ai casi in cui il pubblico ministero aveva richiesto l'autorizzazione nell'ambito di indagini per reati diversi da quelli previsti dall'art. 132 codice *privacy*.

Ciò non significa auspicare una rinuncia alle garanzie in un'ottica efficientista, ma ritenere che l'efficienza non possa essere ristretta a causa di una tutela prevalentemente formale[66].

Non sfugge, poi, la sproporzione: l'acquisizione del dato di posizionamento non è presidiato da alcuna garanzia se avviene tramite localizzazione satellitare; diversamente, se raccolto *ex* art. 132 codice *privacy*, il medesimo dato richiede l'autorizzazione del giudice. Si ribadisce che si tratta della stessa tipologia di dato di localizzazione, senza che entri in alcun modo in gioco, in entrambi i casi, il contenuto comunicativo.

La tutela rafforzata stride ancor più non appena si consideri che le persone, più o meno consapevolmente, cedono costantemente i dati di localizzazione a società che le profilano, al solo fine di poter fruire di servizi internet, anche del tutto superflui, dimostrando incuranza nella protezione dei loro dati di ubicazione.

Infine, in tema di dati di localizzazione dei dispositivi mobili occorre porre in luce un ulteriore aspetto. La *data retention* attiene ai dati di traffico che attengono a una comunicazione. Si tratta allora di capire quale sia la disciplina dei dati generati dai dispositivi a prescindere dal fatto che in quel momento sia in essere una comunicazione.

Secondo il Garante tali dati sfuggirebbero alla disciplina dell'art. 132 codice *privacy*, con la conseguente possibilità di acquisirli anche in assenza di una autorizzazione del giudice per le indagini preliminari[67]. Dal canto suo, la dottrina che ha colto tale sottile profilo, aveva precisato come, alla luce degli artt. 126 e 127 d.lgs. 30 giugno 2003 n. 196, «il codice per la protezione dei dati personali consente il trattamento dei dati relativi all'ubicazione anche se diversi da quelli inerenti al traffico»[68].

---

[66] Invero ciò riflette un fenomeno più generale, dato che «non si può seriamente asserire che tutte le forme note e attuali del 'rituale' siano *ex se* latrici di valori e garanzie, e in quanto tali immodificabili»: B. GALGANI, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale 'virtuoso'*, Milano, 2022, p. 263.

[67] Si veda Garante per la protezione dei dati personali, Provvedimento del 19 dicembre 2008, *Persone disperse in montagna: si può localizzare il cellulare per rintracciarle*.

[68] In questi termini, G. DI PAOLO, *Acquisizione dinamica dei dati relativi all'ubicazione del cellulare e altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense*, cit., p. 223. Al riguardo, cfr. anche A. CA-

12. Conclusioni: verso il superamento della parallasse percettiva nel bilanciamento delle garanzie

Nel sistema attuale, la localizzazione può essere ottenuta attraverso mezzi di ricerca della prova e mezzi di prova.

Si è già ricordato come nell'alveo dell'art. 189 c.p.p. vengano ricondotti sia il pedinamento 'classico' sia la localizzazione satellitare e come essi non richiedano di regola né l'autorizzazione del pubblico ministero[69] né l'autorizzazione di un Gip, salvo il caso in cui entri in gioco la violazione del domicilio o, per il pedinamento, la captazione di contenuto comunicativo.

Diversamente, ai sensi dell'art. 132 codice *privacy*, i dati di ubicazione derivanti da traffico telefonico, telematico e delle chiamate senza risposta possono essere acquisiti solo in forza di un decreto motivato del giudice.

L'asimmetria tra, da un lato, la disciplina della localizzazione satellitare e del pedinamento e, dall'altro, quella dei dati di ubicazione esterni alle comunicazioni emerge anche in rapporto a un ulteriore profilo. Infatti, nei primi due casi, i dati di localizzazione possono essere raccolti a prescindere dal tipo di reato perseguito, salvo il rispetto del principio di proporzionalità; invece, nell'ipotesi dei c.d. tabulati, l'acquisizione dei dati di localizzazione non solo deve essere rilevante ai fini delle indagini, ma è circoscritta ai soli casi in cui sussistano

> «sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi».

Si noti, poi, che i dati di localizzazione possono trovare ingresso nel procedimento penale come documenti[70] (si pensi, ad esempio, alla acquisizione dalla mappa degli spostamenti di *Google Maps*) o in forza di

---

MON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005, 2, pp. 631-632.

[69] Altro discorso è, infatti, che gli stessi possano essere delegati *ex* art. 370 c.p.p.

[70] In tema, cfr. Cass. pen., sez. VI, sent. 17 maggio 2022 n. 25555.

una consulenza tecnica o perizia, come potrebbe accadere nell'ipotesi in cui sia necessario ricavare dai dati digitali *Exif* di una fotografia il luogo in cui la stessa è stata scattata.

Poiché la raccolta del dato di localizzazione pare determinare la medesima incidenza sul piano dei diritti fondamentali a prescindere dal mezzo impiegato, ci si può chiedere quale sia la *ratio* di garanzie così diversamente modulate a seconda della disciplina che venga di volta in volta in rilievo. Forse, se l'ingerenza è la medesima, *ex* art. 3 Cost. sarebbe opportuno che pure la garanzia fosse la medesima. Si può inoltre aggiungere come le medicine abbiano un effetto curativo solo se assunte nel giusto dosaggio. Diversamente, se somministrate in eccesso, possono provocare effetti collaterali.

Invero, in tema di tutele, da un lato, si assiste a rifluenze inquisitorie, che propugnano la riduzione delle garanzie, specie in presenza di reati gravi e che vanno rifuggite se non altro perché sussiste la presunzione di non colpevolezza. Dall'altro lato, si registrano delle posizioni di eccessivo garantismo, che rischiano di paralizzare il sistema.

Occorre ricordare come la prospettiva con cui osserviamo la realtà possa far mutare ciò che vediamo, come dimostra il fenomeno della parallasse. In effetti, in tema di garanzie, il dibattito appare sbilanciato[71] perché muove o da un approccio securitario o dall'esigenza di tutelare il diritto al rispetto della vita privata, dimenticando che esistono anche altri diritti in gioco, di cui dovrebbe invece tenere conto una più adeguata calibratura della disciplina.

In particolare, anzitutto, il bilanciamento deve prendere in considerazione l'art. 112 Cost. che postula il principio dell'obbligatorietà dell'esercizio dell'azione penale. Tuttavia, per poter attuare tale principio, il pubblico ministero deve essere messo in grado di ricercare gli elementi di prova a favore e a carico dell'indagato, senza eccessivi ingessamenti, con conseguente limitazione delle richieste di autorizzazione ai soli casi di effettiva marcata ingerenza sul piano dei diritti fondamen-

[71] Proprio in riferimento alla localizzazione, a seguito della sentenza Carpenter c. United States, O.S. KERR, *Implementing Carpenter. The digital fourth amendment*, in *USC Law Legal Studies Paper* No. 18-29, 2018, rimarca la necessità di «equilibrium-adjustment principles».

tali, anche nell'ottica di non sovraccaricare ulteriormente i giudici per le indagini preliminari.

In secondo luogo, non deve essere pretermesso il diritto di difesa. Invero i dati di localizzazione possono essere funzionali a dimostrare l'estraneità ai fatti dell'indagato/imputato, senza contare l'importanza che essi possono rivestire per far acclarare che il falso testimone si trovava in luogo diverso da quello in cui dichiara di essersi trovato.

Inoltre, una adeguata calibratura dovrebbe considerare anche la tutela della vittima. A lungo marginalizzata nel nostro sistema, viene invece presa in considerazione da taluni atti dell'Unione europea[72], costringendo il legislatore nazionale a interrogarsi sul ruolo a essa riservato. Invero, se le tutele offerte a Caino sono traguardo di civiltà rispetto alle quali non si può e non si deve arretrare, il cammino per la tutela effettiva di Abele[73] si profila ancora lungo e in salita.

In conclusione, a fronte di un approccio volto a valorizzare unidirezionalmente la *privacy*[74], occorre ricordare come sia invece lo stesso Garante per la protezione dei dati personali ad assumere posizioni più equilibrate, ricordando anche, in tema di localizzazione, che la *privacy* può essere un diritto recessivo rispetto ad altri diritti[75].

---

[72] Al riguardo, sembra opportuno ricordare anzitutto la Direttiva 2012/29/UE del 25 ottobre 2012 che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GA.

[73] Invero, nell'attuale sistema giuridico, la vittima riceve ancora una scarsa tutela effettiva, subendo non di rado anche una vittimizzazione secondaria, senza contare il sacrificio economico richiestole per sostenere i costi difensivi ed i riverberi sul piano personale e professionale derivanti dallo svolgimento del processo penale che la vede persona offesa. Per un approfondimento sulla marginalizzazione della vittima, si rinvia a M. BARGIS, H. BELLUTA (a cura di), *Vittime di reato e sistema penale. La ricerca di nuovi equilibri*, Torino, 2017; nonché V. PATANÈ, *Tutela della vittima*, in *Diritti della persona e nuove sfide del processo penale*, cit., p. 339 ss.

[74] Il che si pone in «un moto 'controcorrente' rispetto a salvaguardie più 'classiche' del rito penale (si pensi solo al diritto al confronto con l'accusatore e all'assistenza tecnica di un difensore) che invece attraversano una fase, per così dire, recessiva, testimoniata dalla più recente giurisprudenza di Strasburgo». In questi termini, cfr. L. LUPÁRIA DONATI, in *Diritti della persona e nuove sfide del processo penale*, cit., p. 98.

[75] Al riguardo, cfr. Provvedimento 22 gennaio 2015, n. 32 (doc. web. n. 3736199), *Utilizzo di tecnologie di geolocalizzazione di persone infortunate o disperse in montagna da parte del Corpo Nazionale Soccorso Alpino e Speleologico (CNSAS)*.

LE OPERAZIONI SOTTO COPERTURA NEL *WEB*

Pasquale Bronzo

SOMMARIO: *1. Indagini* undercover. *2. L'agente sotto copertura nel* cyberspazio. *3. Resa processuale. 4. Violazione delle procedure. 5. Presidi di garanzia. 6. Il d.l. 10 agosto 2023 n. 105: un* Covert Cyber Operation Act*?*

1. Indagini undercover

Tra le trasformazioni più rilevanti che, da qualche decennio ormai, stanno attraversando il nostro sistema processuale – e non solo il nostro – possiamo annoverare lo sviluppo di regole speciali volte a disciplinare modalità investigative ritenute necessarie per contrastare efficacemente forme particolarmente allarmanti di criminalità. Si parla di "speciali tecniche di indagine": la caratterizzazione in chiave di specialità rimanda ad un ambito applicativo ridotto entro margini di stretta necessità, e dall'altro a modalità di accertamento la cui particolarità è contrassegnata dalla spiccata invasività nei diritti individuali. La carica invasiva, connessa alla *insidiosità* delle attività in discorso, invisibili a chi le subisce, risulta potenziata quando – come sempre più spesso accade – esse si avvalgono di strumenti tecnologicamente avanzati o si svolgono nella rete *internet* anziché nel mondo fisico[1].

Questa intrusività pone l'ineludibile esigenza di sorvegliare le garanzie di libertà da possibili tendenze involutive della normazione e della prassi, specie nelle fasi iniziali del procedimento. La sfida che il nostro ordinamento si trova oggi ad affrontare non è più soltanto quella di garantire il binomio "efficacia investigativa – tutela del diritto di di-

[1] Le speciali tecniche di indagine oggi partecipano della delicatezza di tutte le nuove tecnologie del controllo (cfr. G. DI PAOLO, *Tecnologie del controllo e prova penale. L'esperienza statunitense e spunti per la comparazione*, Padova, 2008, p. 3 ss.)

fesa", essendo necessario, invece, preservare i diritti individuali di chiunque sia convolto dall'esercizio del potere investigativo[2].

Tra le tecniche speciali di indagine la più controversa, e quella di uso più risalente, viene sinteticamente definita 'operazione sotto copertura': una persona – ufficiale di polizia o privato cittadino – celando la propria identità, si infiltra all'interno di tali associazioni allo scopo di scoprirne la struttura, individuare i partecipanti, procacciare prove. Questa metodica investigativa consente di penetrare surrettiziamente in organizzazioni che, in determinati settori della criminalità, si sono manifestate impenetrabili con gli ordinari strumenti d'indagine.

Le operazioni sotto copertura costituiscono metodi di indagine dai tratti fortemente anomali: sia perché comprendono condotte che, al di fuori dell'eccezionale contesto esimente, integrerebbero la responsabilità penale dell'operatore, sia perché la loro insidiosità – connessa alla circostanza che chi agisce non viene percepito dall'indagato come "autorità procedente" – implica un inevitabile sacrificio delle garanzie difensive, *in primis* il diritto al silenzio, altrimenti riconosciute alla persona sottoposta a indagine rispetto a coloro che siano espressione di poteri pubblici.

Il primo sviluppo di questa metodica investigativa si registra oltreoceano intorno ai primi del Novecento nella repressione della corruzione pubblica, e a quel suo successo deve la sua diffusione su scala globale, ma la declinazione europea si distacca decisamente dal modello americano delle *covert investigations*.

Negli Stati Uniti le operazioni sotto copertura sono assai poco regolamentate, soprattutto quanto ai possibili contenuti, e, in secondo luogo, quel che è più interessante notare è che è pacificamente ammessa la figura dell'agente provocatore; coerentemente, non è mai punibile il *police incitement*, ossia la condotta di chi eserciti sulla persona indagata un'influenza tale da indurla a impegnarsi in un reato che altrimenti non avrebbe commesso (le chiamano *sting operations*). L'imputato, soggetto passivo di questo tipo di indagini, è però ammesso a dimostrare la provocazione in base a una sorta di inversione dell'onere della prova:

[2] Cfr. R. ORLANDI, *Postulati del processo penale contemporaneo tra principi "naturali" e concezioni normative*, in *Riv. it. dir. proc pen.*, 2024, p. 476 ss.

attraverso la c.d. "entrapment defense" guadagna l'assoluzione dimostrando di esser stato indotto o persuaso dall'agenti sotto copertura, a commettere un reato che altrimenti non avrebbe compiuto[3].

In Italia, invece, questa metodica affiora sul piano normativo relativamente tardi, nei primi anni Novanta, ed è caratterizzata da una normazione dettagliata, molto attenta a perimetrare i confini dell'agire investivo mascherato. Più in generale, in tutti i sistemi di *Civil law* sono normativamente disciplinate le operazioni che è consentito effettuare sotto copertura, i reati per l'accertamento dei quali sono consentite (reati particolarmente allarmanti, la cui gravità rende tollerabile la flessione degli *standard* di garanzia), le procedure che devono essere seguite, l'organo, di regola giudiziario, chiamato a vigilare sull'osservanza delle regole da parte dell'organo poliziesco.

Questa differente postura dei diversi ordinamenti nei confronti delle operazioni *undercover* ha a che vedere col recente passato degli Stati europei, in cui l'esperienza dei totalitarismi ha lasciato in eredità un diffuso sospetto nei confronti delle manifestazioni di potere delle forze dell'ordine, dal momento che queste attività sono associate al sociale, alla repressione del dissenso politico, allo Stato di polizia[4].

La creazione di uno 'statuto generale' delle operazioni sotto copertura in Italia si deve alla l. 16 marzo 2006 n. 146, emanata in attuazione della Convenzione di Palermo contro il crimine organizzato transnazionale: prima di questa novella avevamo un quadro normativo frammentato, nel quale queste tecniche venivano previste e regolate volta per volta in relazione a determinati settori penali[5]. La novella ha consentito

[3] Cfr. J.E. ROSS, *Indagini sotto copertura negli Usa e in Italia: esperienze a confronto*, in *Criminalia*, 2019, p. 61 ss., nonché ID., *Impediments to Transnational Cooperation in Undercover Policing: A Comparative Study of the United States and Italy*, in *Am. J. Comp. L.*, 2004, vol. 52, p. 581 ss.

[4] Cfr. B. FRAGASSO, *L'estensione delle operazioni sotto copertura ai delitti contro la pubblica amministrazione: dalla giurisprudenza della Corte EDU, e dalle corti americane, un freno allo sdoganamento della provocazione poliziesca*, in *Sistema penale* (rivista web), 5 marzo 2019 (ultimo accesso il 28 febbraio 2025).

[5] Il prototipo italiano è costituito dalla previsione dell'acquisto simulato di stupefacenti di cui all'art. 97 d.P.R. 9 ottobre 1990 n. 309 (cfr. L. RISICATO, *L'acquisto simulato di droga nell'ambigua cornice dell'agente provocatore*, in *Riv. it. dir. proc. pen.*, 1994, p. 1592) nella quale il legislatore, concentrato sugli aspetti sostanziali dell'istitu-

di raccogliere all'interno di un'unica disciplina (o quasi) il regime giuridico di tutte le operazioni sotto copertura consentite dal nostro ordinamento, con conseguente abrogazione di gran parte delle normative speciali anteriori.

Negli anni l'ambito normativo di applicazione dell'istituto a fini di indagine penale ha visto una ulteriore «escalation»[6]: la l. 9 gennaio 2019 n. 3 l'ha esteso a buona parte dei delitti contro la pubblica amministrazione[7]; la l. 9 marzo 2022 n. 22 l'ha previsto per la repressione del commercio illegale di beni culturali[8]; la l. 27 dicembre 2023 n. 206, ha fatto altrettanto per i reati di contraffazione in campo agroalimentare[9]. Da ultimo, un decreto-legge del 2023 si è occupato delle indagini sotto copertura in ambiente digitale in relazione ai «delitti commessi con finalità di terrorismo o di eversione» e ai «reati informatici commessi ai danni delle infrastrutture critiche informatizzate individuate dalla normativa nazionale e internazionale»[10].

Complessivamente, eccettuando le spiccate peculiarità della disciplina in materia di reati pedopornografici[11], possiamo dire di avere oggi

---

to, trascurava i profili procedimentali. La figura negli anni immediatamente successivi è stata poi riprodotta, con le medesime caratteristiche strutturali, ai reati in tema di immigrazione, di armi, di terrorismo e, con alcune peculiarità procedurali, di pedopornografia (G. BARROCU, *Le indagini sotto copertura*, Napoli, 2011, p. 20 ss.).

[6] Cfr. M. BIRAL, *La testimonianza anonima degli agenti sotto copertura*, Milano, 2023, p. 114.

[7] Cfr. F. CASSIBBA, *L'espansione delle operazioni sotto copertura*, in C. IASEVOLI (a cura di), *La c.d. legge "spazzacorrotti"*, Bari, 2019, p. 199 ss.

[8] Cfr. M. FUSAROLI, *I nuovi scenari delle attività investigative riguardanti i fenomeni criminosi connessi al* cultural heritage. *Un primo bilancio sulle ripercussioni processuali delle novità apportate dalla legge n. 22 del 2022 alla materia della tutela penale dei beni culturali*, in *Cass. pen.*, 2024, p. 392 ss.

[9] L. 27 dicembre 2023 n. 206, recante: «Disposizioni organiche per la valorizzazione, la promozione e la tutela del Made in Italy» (cfr. A. NATALINI, *Dop e Igp agroalimentari contraffatti, estese le operazioni sotto copertura (L. 206/2023)*, in *Guida dir.*, 2024, 4, p. 64 ss.).

[10] *Infra*, par. 6.

[11] Per l'accertamento di questi reati si prevede che vengano impiegate «indicazioni di copertura, anche per attivare siti nelle reti, realizzare o gestire aree di comunicazione o scambio su reti o sistemi telematici, ovvero per partecipare a esse» (art. 14 comma 2 l. 3 agosto 1998, n. 286). Sulle peculiarità di questa sotto-fattispecie, la più significativa

un *modello unificato* di 'operazione sotto copertura' piuttosto che specifiche modalità d'azione sagomate in base alle esigenze investigative che caratterizzano i diversi fenomeni criminosi.

Il progressivo ampliamento dell'area applicativa dell'istituto, se per un verso ne attesta la formidabile proficuità, per altro verso lo allontana fatalmente dalla logica di eccezionalità e residualità nella quale è nato. Sempre più spesso la previsione della possibilità di impiegare la tecnica operazioni mascherate risulta giustificata più dalla alta resa del metodo che dalla sua necessarietà, intesa come inidoneità di metodiche di indagine meno insidiose. Accade via via che ci si allontani dalle figure del narcotraffico o delle organizzazioni mafiose e terroristiche, verso fenomenologie criminose che presentano una assai più modesta attitudine al compimento di reati in forma organizzata, senza neppure quelle particolari caratteristiche di complessità e di impenetrabilità attraverso i mezzi di indagine ordinari, che sono proprie dei contesti tradizionali di applicazione: si pensi all'estensione, ad opera della l. 9 marzo 2022 n. 22, delle attività sotto copertura ai reati di traffico di beni culturali.

A volte si ha l'impressione di mosse poco più che simboliche: è il caso della l. 23 dicembre 2023 n. 206 a tutela del c.d. *made in Italy*, la quale consente operazioni mascherate per raccogliere prove in ordine al delitto di «contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari», punito «con la reclusione fino a due anni e con la multa fino a euro 20.000»[12].

---

delle quali è costituita dalla necessaria «richiesta» dell'autorità giudiziaria «motivata a pena di nullità» cfr. P. TROISI, *Le investigazioni digitali sotto copertura*, Bari, 2022, p. 57 ss. È ovviamente peculiare anche la disciplina delle indagini sotto copertura consentite – a fini di *intelligence* – ai componenti dei servizi di sicurezza dalla l. 3 agosto 2007 n. 124.

[12] Qui sono particolarmente evidenti le «ragioni di rappresentazione simbolica dell'efficacia delle politiche repressive dello stato» (G. MELILLO, *Le operazioni sotto copertura nelle indagini relative a delitti con finalità di terrorismo*, in G. DI CHIARA (a cura di), *Il processo penale tra politiche di sicurezza e nuovi garantismi*, Torino, 2003, p. 41).

Per altro verso, sembrerebbe incrinare la ragionevolezza dell'assetto il mancato inserimento tra i reati-presupposto del delitto di associazione per delinquere e di associazione di stampo mafioso di cui agli artt. 416 e 416-*bis* c.p. Fosse davvero così, le organizzazioni criminali per antonomasia resterebbero fuori dall'ambito applicativo di uno

Il rischio di fondo è la «trasmutazione poliziesca»[13] del processo, la penetrazione delle logiche di controllo sociale nel rito penale, il peso abnorme della fase investigativa, straordinariamente potenziata nella sua efficacia, sulle sorti dell'accertamento[14].

Anche nei contenuti questa metodica investigativa appare oggi assai diversa rispetto agli archetipi. Da un lato, appaiono ridimensionate le finalità normativamente consentite: nei sistemi di *civil law* è attualmente recessiva la declinazione *sub specie* di "agente provocatore", cioè di colui che non si limita a infiltrarsi nell'associazione (c.d. "agente infiltrato"), ma determina altri nella commissione di un reato.

Dall'altro lato, questo metodo di indagine ha conosciuto importantissimi aggiornamenti nelle tecniche, che ne hanno notevolmente potenziato l'efficacia. La penetrazione nelle reti criminali, infatti, avviene ormai frequentemente in ambiente digitale perché il *web* è sempre più spesso teatro o strumento di condotte delittuose, tanto che alcuni settori di attività delinquenziali si sono praticamente "trasferiti" sulle piattaforme digitale.

Le nuove "tecnologie dell'informazione e della comunicazione" hanno prodotto profonde trasformazioni sociali, agevolando non solo lo

---

strumento pensato per penetrare all'interno delle reti criminali. In realtà, siccome l'art. 9 co. 8 l. n. 146/2006 prevede tra i destinatari della comunicazione di avvio il procuratore nazionale antimafia «per i delitti indicati all'art. 51, co. 3-*bis*» c.p.p., si potrebbe ritenere che l'omessa menzione degli art. 416 e 416-*bis* c.p. nel comma 1 sia il frutto di una svista (così G. AMARELLI, *Le operazioni sotto copertura*, in V. MAIELLO (a cura di), *I reati in materia di criminalità organizzata*, Torino, 2015, p. 180). Ritiene che i reati in discorso siano fuori dall'ambito applicativo delle operazioni sotto copertura A. CISTERNA, *Attività undercover: quel difficile incontro con il contrasto alla mafia*, in *Guida dir*., 2023, 41, p. 51.

[13] D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Archivio penale*, 2016, 1, p. 46.

[14] Da un diverso punto di vista, è stato segnalato come l'estensione dello strumento alle indagini relative a reati che possono avere facilmente struttura bilaterale e non già associativa come è accaduto per la corruzione, aumenti il rischio che l'attività *undercover*, lungi dall'esaurirsi in contegni meramente passivi, si traduca in condotte di istigazione o provocazione, le uniche davvero in grado di far emergere il fenomeno corruttivo (A. CAMON, *Disegno di legge spazzacorrotti e processo penale. Osservazioni a prima lettura*, in *archiviopenale.it* (rivista web), 5 novembre 2018, p. 3 ss., ultimo accesso il 28 febbraio 2025).

scambio di saperi ma anche la creazione di nuovi spazi di vita nei quali si manifestazione un gran numero di esperienze umane[15]; in questi spazi virtuali abbondano occasioni per delinquere prima inesistenti e modalità totalmente nuove per commettere i reati.

Nell'anonimato del *web* – e ancor più nel *deep web*, i cui contenuti non sono indicizzati nei motori di ricerca – si può organizzare facilmente un attentato terroristico o un traffico illecito di qualsiasi natura, riciclare qualsiasi capitale illecito attraverso crypto-valute[16]. Le investigazioni penali, di fronte a questo scenario, sono dovute scendere sullo stesso terreno, trasponendo nella realtà virtuale le tecniche dell'infiltrazione mascherata[17].

2. L'agente sotto copertura nel cyberspazio

Le attività svolte *undercover* nell'ambiente informatico partecipano, ovviamente, di tutti i profili di delicatezza propri delle altre operazioni sotto copertura, ma qualche criticità, quando le infiltrazioni avvengono nel mondo digitale, risulta addirittura acutizzata[18]. Nel nostro ordinamento, infatti, l'istituto deve sottostare a due limiti fondamentali, i quali, tuttavia, sono entrambi facilmente superabili quando si opera sul *web*: in primo luogo, l'inammissibilità di impiego a fini preventivi; in secondo luogo, l'inammissibilità della figura investigativa dell'agente provocatore.

Il primo limite deriva dalla configurazione normativa delle "operazioni", che sono un "mezzo di ricerca della prova" e non possono essere

[15] L. PICOTTI, *I diritti fondamentali nell'uso e abuso dei* social network*. Aspetti penali*, in *Giur. merito*, 2012, p. 2522 ss.

[16] R.M. VADALÀ, *Criptovalute e* cyberlaundering*: novità antiriciclaggio nell'attesa del recepimento della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, in *Sistema penale* (rivista web), 6 maggio 2020 (ultimo accesso il 28 febbraio 2025). Cfr. anche il contributo di J. DELLA TORRE nel presente volume.

[17] D. CURTOTTI, *Operazioni sotto copertura*, in B. ROMANO (a cura di), *Le associazioni di tipo mafioso*, Torino, 2015, p. 431.

[18] La delicatezza che da sempre caratterizza il mascheramento delle indagini viene a cumularsi a quella propria della 'prova informatica' (cfr. G. DI PAOLO, *Prova informatica*, in *Enc. Dir.*, *Annali*, VI, Milano, 2007, p. 736 ss.).

utilizzate per procacciare notizie di reato: esse, cioè non possono avere funzione meramente esplorativa ma devono inserirsi in un procedimento penale già instaurato. Nel nostro sistema, infatti, non sono ricavabili spazi per un impiego di queste attività come strumenti di prevenzione: non a caso sia l'art. 97 d.P.R. n. 309 del 1990, prima configurazione normativa, sia l'art. 9 l. n. 16 marzo 2006 n. 146, che contiene oggi lo statuto generale le descrivono come attività compiute «al solo fine di acquisire elementi di prova» in ordine ai delitti indicati.

Allora, l'obbligo di comunicare al pubblico ministero le modalità delle operazioni e i relativi risultati, la natura "eccezionale" delle operazioni in parola, le univoche indicazioni provenienti dalla dottrina e dalla giurisprudenza nazionale, secondo la quale le ingerenze investigative nei diritti fondamentali di regola presuppongono una *notitia criminis*, e quelle altrettanto chiare provenienti dalla giurisprudenza europea, che vincolano il compimento di tali indagini all'esistenza di una attività criminosa conclusa o *in itinere*, sono elementi che portano a estromettere tali operazioni dall'area delle attività di polizia di sicurezza.

E tuttavia, il confine tra prevenzione e repressione è fatalmente destinato ad assottigliarsi: ciò dipende essenzialmente da due fattori. Se uno è legato alla funzionalità dell'istituto a indagare sul crimine organizzato – l'«infiltrazione» di agenti all'interno delle organizzazioni criminali è strumentale (anche) alla ricerca di notizie di reato in relazione alla fisionomia dell'associazione, ai suoi membri, e ai futuri progetti criminosi – l'altro è invece connesso, per l'appunto, al contesto digitale delle attività *under cover*.

In generale, le c.d. "indagini digitali"[19] offrono la possibilità di svolgere facilmente attività di sorveglianza segreta e continua, e consentono raccolte massiva di informazioni, il che le rende naturalmente adatte a una duplice funzione, preventiva e repressiva insieme[20]. La loro attitudine esplorativa ne fa lo strumento elettivo delle attività di *intelligence* criminale basate sull'analisi di informazioni variamente raccolte che si pongono l'obiettivo di identificare minacce e scongiurare il compimen-

[19] S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 43.

[20] D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, cit., p. 52.

to di fatti di reato quando sussista un fondato sospetto di incombente realizzazione[21].

Quando l'investigazione nella realtà virtuale avviene attraverso un'operazione sotto copertura (in relazione alla quale l'impiego a fini preventivi è normativamente escluso) è proprio la conformazione del c.d. *cyberspazio* e il modo in cui in esso tutti noi ci muoviamo, a favorire le distorsioni applicative: l'inserimento di agenti *undercover* in una *chat-line* è fisiologicamente strumento adatto a captare informazioni concernenti possibili crimini futuri più che a reperire elementi di prova riguardo a reati già commessi.

È facile allora che l'indagine diventi occasione per testare la propensione a delinquere delle persone-bersaglio o intercettare *hotspot* di criminalità, secondo una metodica che gli americani chiamano *manna from heaven operations*, nelle quali le quali la polizia lascia, per esempio, incustoditi oggetti di valore in luoghi pubblici per tentare i passanti[22].

Il secondo importantissimo limite dell'istituto delle operazioni sotto copertura riguarda il discrimine tra "agente infiltrato" e "agente provocatore": come già ricordato, nel nostro sistema le indagini sotto copertura non possono costituire condotte di provocazione; l'istituto presuppone contegni passivi o comunque produttivi di forme di compartecipazione materiale, mai condotte capaci di ingenerare propositi criminosi che, in loro assenza, non sarebbero venuti alla luce[23].

E tuttavia, il confine tra contegno passivo e contegno proattivo, incerto sempre, lo è massimamente quando condotte criminose e atti di indagine si svolgono in uno spazio virtuale. Le metodiche tipiche delle

---

[21] Indagini 'proattive', nella definizione della Risoluzione del XVIII Congresso internazionale di diritto penale, Istanbul, 20-27 settembre 2009, in *Riv. dir. process.*, 2010, 333 ss.

[22] Le 'operazioni manna dal cielo' sono una tipica indagine proattiva non soggettivamente indirizzata verso individui o gruppi determinati: cfr. G. ROBERTSON, *Entrapment Evidence: Manna from Heaven, or Fruit of the Poisoned Tree?*, in *Criminal Law Review*, 1994, p. 805 ss., che riporta il *leading case Williams v. DPP* del 1994.

[23] Chiara sul punto anche la giurisprudenza della Corte europea: v. per tutti Corte eur. dir. uomo, sent. 9 giugno 1998, Teixeira de Castro c. Portogallo, §§ 35-36 e 39; nonché, in relazione alla disciplina italiana, Corte eur. dir. uomo, sez. I, sent. 21 marzo 2002, Calabrò c. Italia e Germania (cfr. F. CASSIBBA, *L'espansione delle operazioni sotto copertura*, cit., p. 206 ss.).

operazioni *undercover* digitali lambiscono infatti costantemente la provocazione: l'attivazione di siti civetta, la realizzazione di aree di *sharing*, la diffusione *on-line* di materiale pedopornografico, creano artificiosamente piazze di scambio virtuali in grado di attrarre potenziali criminali e conducono i frequentatori di un gruppo o di una piattaforma a scaricare tale materiale, commettendo reato o a caricarne altro a loro volta. Pertanto, si tratta di attività fatalmente propositive.

A determinare questo scivolamento dell'infiltrazione verso il *police encitement* è la peculiarità della rete internet, che consente a qualsiasi navigante di essere chiunque e rappresentarsi nei più diversi modi: rende bene l'idea una famosa vignetta apparsa su un magazine americano nel 1993, nella quale è ritratto un cane, seduto alla scrivania che naviga al computer come se fosse una persona, che dice all'altro cane seduto per terra che lo osserva perplesso: *on the internet, nobody knows you're a dog*[24].

L'agente sotto copertura digitale è in grado di «indossare i panni dell'esca "ideale" per il bersaglio, impersonando, a seconda dell'occorrenza, conoscenti, familiari, estranei»[25], avendo buon gioco in qualsiasi manipolazione.

In più, dobbiamo considerare che, rispetto alle tecniche di infiltrazione tradizionali, l'ambiente digitale potenzia l'efficacia degli adescamenti, perché nel *web* la percezione dell'illegalità si attenua: i criminologi hanno notato che il *cyberspazio* influisce sulle modalità percettive e cognitive delle persone, riduce gli ordinari freni inibitori presenti che si attivano nelle relazioni fisiche, contribuendo a sfumare i confini già labili tra conformità, devianza e criminalità; né vale granché adoperare "maschere di deterrenza", che avvisano i navigatori del *web* che il contenuto del sito è vietato dalla legge; colpa, dicono i cyber criminologi,

[24] R. LINCOLN, I.R. COYLE, *No-one Knows You're a Dog on the Internet: Implications for Proactive Police Investigation of Sexual Offenders*, in 20 *Psychiatry, Psychology and Law*, 2013, p. 294 ss. L'immagine è richiamata da S. CIAMPI, *Legge n. 137/2023 e investigazioni (digitali) sotto copertura: la cedevolezza del "modello sostanzialista", l'assenza di uno statuto processuale, la necessità di una rivoluzione copernicana nell'approccio alla materia*, in *Processo penale e giustizia*, 2024, 3, p. 734.

[25] P. TROISI, *Le investigazioni digitali sotto copertura*, cit., p. 193.

dell'«anonimato dissociativo» generato dalla rete, consentendo di separare la propria identità dall'esternazione dei propri contenuti[26].

3. Resa processuale

Nel nostro sistema sono numerosi i problemi relativi al trattamento processuale di queste operazioni: ciò si deve anche al fatto che la disciplina italiana, a differenza di omologhi stranieri, se è molto attenta a definire i confini della non punibilità delle condotte dell'infiltrato e alla tutela della sua incolumità, anche ai fini del suo possibile reimpiego[27], lo è assai molto meno alle implicazioni processuali di questa metodica investigativa.

Alcune complicazioni riguardano la *spendibilità* processuale dei risultati di queste indagini: se non pongono particolari questioni la raccolta di prove reali dei reati e l'acquisizione dei relativi proventi (le "consegne controllate" e il "ritardo nei sequestri" hanno costituito la funzione principale delle attività mascherate già nella prima figura in materia di traffico di stupefacenti), assai problematico, invece, risulta l'apporto dichiarativo dell'agente *undercover* nel processo.

Non è cosa da poco: il profitto processuale di queste attività mascherate non si limita, come si potrebbe pensare, ad arresti o al sequestro di prove reali o corpi di reato[28]; avviene invece frequentemente che vengano acquisite in dibattimento, dalla voce dell'operante, informazioni raccolte durante e grazie alle operazioni in parola: «dopo tutti i rischi intrapresi e le energie impiegate, sarebbe […] singolare limitare il recu-

[26] Cfr. K. JAISHANKA, *Establishing a Theory of Cyber Crimes*, in 1 *International Journal of Cyber Criminology*, 2007, 2, p. 7 ss. rileva come i comportamenti umani subiscano enormi variazioni nel passaggio tra lo spazio fisico e quello virtuale: persone che presentano un comportamento criminale represso all'interno dello spazio fisico rivelano la propensione a commettere, nel mondo digitale, azioni criminali che, in considerazione del loro status o della loro posizione sociale, non avrebbero mai commesso nel mondo reale.

[27] Cfr. M. BIRAL, *La testimonianza anonima*, cit., p. 153.

[28] Né è trascurabile peso della documentazione dell'attività mascherata in sé: ne resta traccia nelle annotazioni previste dall'art. 115 comma 1-*bis* disp. att. c.p.p., fruibili probatoriamente nei riti premiali.

pero del sapere acquisito dall'infiltrato durante la sua attività al solo sequestro del materiale», si osserva[29].

L'esame dell'agente *undercover* in realtà può servire in chiave accusatoria come difensiva, e può persino essere utile alla verifica della correttezza dell'operante, per escludere condotte istigatorie[30]. Ai sensi dell'art. 497 co. 2-*bis* c.p.p., gli agenti che hanno effettuato attività mascherate chiamati a deporre, «invitati a fornire le proprie generalità, indicano quelle di copertura utilizzate nel corso delle attività medesime»[31]; l'esame avviene dunque in modo 'schermato', quanto meno agli occhi della difesa e del giudice (solo il p.m. può chiedere di conoscere la reale identità, ai sensi dell'art. 9 co. 4 l. 146/2006); e il dichiarante sotto pseudonimo può non essere un funzionario di polizia, ma un privato utilizzato dagli inquirenti come interposto[32].

Le ridotte possibilità di verifica dell'affidabilità della prova dichiarativa pongono questa disciplina – il cui difetto principale risiede nell'automatismo dello schermo, a prescindere dall'esistenza in concreto

[29] A. SUTERA SARDO, *Aspetti processuali dell'agente provocatore*, in R. MINNA, A. SUTERA SARDO, *Agente provocatore. Profili sostanziali e processuali*, Milano, 2003, p. 135. L'agente infiltrato può assumere tanto la qualifica di testimone, quanto quella di imputato o imputato in procedimento connesso: dipende dalla circostanza che siano state rispettate oppure no le procedure previste; nel primo caso egli, risultando non punibile assume il ruolo di testimone nel processo a carico dell'imputato; nel secondo caso, al contrario, ravvisandosi nel suo comportamento un fatto penalmente rilevante, assume la figura di coimputato o di imputato in procedimento connesso o collegato. La diversa qualifica processuale incide sul regime di acquisizione e impiego decisorio dichiarazioni, e sulla applicabilità o no del combinato disposto degli artt. 210 e 193 co. 3 e 4 c.p.p. (Cass. pen., sez. II, sent. 28 maggio 2008 n. 38488, in *Cass. pen.*, 2009, p. 2958).

[30] Cfr. M. BIRAL, *La testimonianza anonima*, cit., p. 128, segnala come nella giurisprudenza della Corte di Strasburgo è molto valorizzato lo spazio concesso alla difesa, anche attraverso il controesame dell'infiltrato, nel c.d. *entrapment plea*.

[31] Interpolato dall'art. 8 l. 13 agosto 2010 n. 136. Non c'è in realtà un autentico anonimato, ma una relativa segretezza: solo il pubblico ministero può pretendere di conoscere il nominativo reale dell'operante.

[32] Il dato richiama un altro profilo di criticità di queste operazioni, comune a tutte le indagini ad alta tecnologia: la sostanziale delega, da parte del pubblico ministero, ai soggetti incaricati di esperire le indagini informatiche nella selezione e nella raccolta delle informazioni sui fatti (G. DI PAOLO, *Prova informatica*, cit., p. 738).

di esigenze di protezione dell'infiltrato – al limite della sostenibilità costituzionale[33].

Il problema potrebbe essere superato, *de iure condendo*, attraverso l'istituzione di un congegno protettivo attivabile dal giudice su richiesta del pubblico ministero, previa verifica della concreta esigenza, conservando il potere di ordinare lo svelamento quando ravvisi cessato il pericolo, o emergano esigenze attinenti alla valutazione di attendibilità della fonte irragionevolmente ostacolate dalla protezione[34].

È dubbio che sia ammissibile la testimonianza *de relato* dell'agente mascherato sulle dichiarazioni apprese nel corso delle attività. C'è chi distingue tra le dichiarazioni provocate (sulle quali non si potrebbe testimoniare) e quelle non provocate: distinzione difficile in pratica, e forse irrilevante ai fini della ratio di tutela della libertà di autodeterminazione processuale dell'indagato[35].

La giurisprudenza di legittimità, dal canto suo, ammette senza riserve la testimonianza indiretta. Non solo. Essa esclude l'applicabilità al medesimo dell'art. 62 c.p.p. che, come è noto, detta un generale divieto di testimonianza *de relato* sulle dichiarazioni comunque rese dall'indagato o dall'imputato all'interno del procedimento, perché – dice la Corte di Cassazione – gli agenti *undercover* sono soggetti partecipanti all'azione e non hanno agito nella veste di ufficiali di polizia giudiziaria con i poteri autoritativi e certificatori connessi alla qualifica[36].

[33] Sui rapporti tra principio del contraddittorio e anonimato del testimone cfr. F. CAPRIOLI, *La tutela del testimone nei processi di criminalità organizzata*, in AA.VV., *Verso uno statuto del testimone nel processo penale*, Milano, 2005, p. 67.

[34] M. BIRAL, *La testimonianza anonima*, cit., p. 210 ss.

[35] L. LUDOVICI, *L'agente sotto copertura*, in G. COLAIACOVO (a cura di), *Sicurezza, informazioni e giustizia penale*, Pisa, 2023, p. 706.

[36] Cass. pen., sez. II, sent. 22 dicembre 2016 n. 14714, Macera, in *C.E.D. Cass.*, n. 269670.

4. Violazione delle procedure

Ancora più delicati sono i problemi processuali legati a operazioni sotto copertura *illegittime*, che a loro volta generano questioni di spendibilità dei risultati.

Per restare in ambito digitale (anche se il problema è generale) l'attivazione di profili di copertura funzionali a stringere contatti telematici o a introdursi in aree virtuali riservate di comunicazione e di scambio è un'attività investigativa oggi normativamente regolata[37], per la quale si pone il problema del trattamento processuale degli esiti informativi di attività condotte violando le regole: perché fuori dai casi consentiti, senza i controlli previsti, o con modalità tali da trasmodare in vera e propria provocazione[38].

Le norme tacciono sul punto: il legislatore del 2006, se ha dedicato attenzione al profilo sostanziale delle operazioni *undercover*, sforzandosi di perimetrare la sfera della non punibilità degli operanti, non ha speso pari impegno nella processualizzazione dell'istituto, trascurando di riprodurre una previsione sanzionatoria del tipo di quella prevista per le intercettazioni all'art. 271 c.p.p. o per le ispezioni presso i difensori all'art. 103, co. 7, c.p.p.; e sebbene la citata novella del 2010 abbia precisato che la violazione delle regole legali preclude l'operatività dello scudo penale[39], la stessa ha omesso qualsiasi specificazione in relazione alle sorti processuali del materiale raccolto nel corso dell'attività abusiva[40].

---

[37] Rispettivamente ai sensi della l. 3 agosto 1998 n. 269 (art. 14-*bis* - 14-*quater*) e del d.l. 19 febbraio 2015 n. 7, conv. in l. 17 aprile 2015 n. 43 (art. 2).

[38] Un problema a parte è rappresentato dal pattugliamento del *web*, attività di indagine che non rientra nello schema delle operazioni sotto copertura anche se è spesso prodromica a quest'ultima (cfr. D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, cit., p. 44-54 e più di recente P. TROISI, *Le investigazioni digitali sotto copertura*, cit., p. 340).

[39] Il comma 1-*bis* dell'art. 9 oggi chiarisce che la causa di giustificazione non si applica «quando le attività non sono state autorizzate e documentate» nelle forme dovute, cosicché il rispetto della procedura è condizione imprescindibile per evitare la punibilità (la scriminante dell'art. 51 c.p. opera entro margini assai ridotti, e non è invocabile quando l'operazione coperta sia stata svolta violando le regole legali).

[40] Non una parola, dunque, nell'art. 9 della legge n. 146/2006, e lo stesso vale per l'art. 14 della legge n. 269/1998 per le operazioni antipedofilia.

In assenza di un dato normativo specifico, dottrina e giurisprudenza hanno affrontato il problema delle conseguenze processuali legate alla violazione della disciplina normativa secondo quattro prevedibili alternative: inutilizzabilità dei risultati probatori in ragione della violazione di una norma penale, inutilizzabilità per violazione della Costituzione (e della Convenzione europea dei diritti dell'uomo), inutilizzabilità per carenza di potere investigativo, irrilevanza delle violazioni ai fini dell'utilizzabilità probatoria delle informazioni.

Una prima impostazione, per affermare la non spendibilità del profitto informativo di operazioni coperte svolte *contra legem*, recupera la tesi secondo cui la "legge rilevante" ai sensi dell'art. 191 c.p.p., include anche le norme penali, e fa discendere l'inutilizzabilità dalla punibilità dell'agente *undercover*, secondo lo schema della "prova illecita". Così nella giurisprudenza di legittimità si afferma che le violazioni della disciplina delle operazioni *undercover* determinano «la responsabilità penale dell'agente infiltrato, e la *conseguente* inutilizzabilità della prova acquisita»[41].

Questa soluzione però è seriamente ipotecata dalla controvertibilità della premessa, quella secondo la quale le norme penali sostanziali possono fungere *ex se* quali regole di esclusione probatoria, eventualmente processualizzate dalla previsione sanzionatoria dell'art. 191 c.p.p.[42].

[41] Cass., sez. VI, sent. 4 febbraio 2020 n. 12204, Giannone, in *CED Cass.*, n. 278730, in motivazione (corsivo nostro). Nello stesso senso Cass. pen., sez. IV, sent. 2 aprile 2015 n. 19122, in *Cass pen.*, 2016. p. 1894, con nota di L. PAOLONI, *La controversa linea di confine tra attività sotto copertura e provocazione poliziesca. Spunti dalla giurisprudenza della Corte edu*; Cass. pen., sez. VI, sent. 30 ottobre 2014 n. 51678, Ursino, in *C.E.D. Cass.*, n. 261449; Cass. pen., sez. III, sent. 7 febbraio 2014, n. 20238, *ivi*, n. 260081 («Quando l'attività concretamente riferibile all'agente sotto copertura o all'interposta persona corrisponde a una o più fra le operazioni espressamente contemplate dal minisistema normativo di riferimento costituito dall'art. 9 l. 16 marzo 2006 n. 146, deve escludersi sia la configurabilità di ipotesi di responsabilità penale a carico di tali soggetti, sia la sussistenza di situazioni di inutilizzabilità della prova acquisita nel corso della indicata attività»).

[42] Cfr. F. CORDERO, *Procedura penale*, IX ed., Milano, 2012, p. 613 ss. Aderiscono all'impostazione F. CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2000, p. 226 ss.; N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Padova, 1992, p. 206 ss.; F.M. GRIFANTINI, voce *Inutilizzabilità*, in *Dig. Pen.*, VII, Torino, 1993, p. 248 ss.; F. PERONI, *Prova illegittima e prova illecita: una singolare nozione di*

Che il profitto probatorio dell'attività coperta debba considerarsi inutilizzabile *perché* frutto di un *police encitement* è un assunto che poggia dunque su basi alquanto malferme.

Per altro verso, vi sarebbero buone ragioni, se volessimo risolvere il problema sulla base della teoria della prova illecita, per estromettere dal materiale utilizzabile per la decisione informazioni raccolte con operazioni mascherate disinvolte che tuttavia non danno luogo ad alcun reato[43].

Una diversa ricostruzione – che sottintende l'adesione alla teorica delle "prove incostituzionali" e/o "anticonvenzionali" – rinviene nell'illegittimità delle operazioni una violazione del diritto all'equo processo *ex* art. 6 Cedu e *dunque* una inutilizzabilità dei relativi prodotti[44]. Questo tuttavia potrebbe dirsi, al più, per il caso in cui l'attività dell'infiltrato abbia integrato un vero e proprio *entrapment* perché solo questa ipotesi porrebbe certamente un problema di iniquità del processo[45]. Assai più difficilmente una tale conclusione potrebbe trarsi in relazione alle operazioni *undercover* effettuate fuori dagli altri presupposti legali (ossia compiute per investigare su reati estranei al catalogo legale, o in assenza delle autorizzazioni e così via), per i quali l'eventuale violazione del diritto al rispetto della vita privata (art. 8 § 2 Cedu) rende *unfair* il processo solo all'esito di una valutazione *complessiva* che riguarda

inutilizzabilità ex *art. 191 c.p.p.*, in *Cass. pen.*, 2005, p. 924 ss.; A. SCELLA, *Prove penali e inutilizzabilità. Uno studio introduttivo*, Torino, 2000, p. 177 ss.

[43] Sulle quali L. PAOLONI, *La controversa linea di confine*, cit., p. 1909; in argomento, cfr. la disamina di P. TROISI, *Le investigazioni digitali*, cit., p. 350. In senso contrario all'impiego dello schema della prova illecita per risolvere il problema delle operazioni mascherate *contra legem*: D. CURTOTTI, *Operazioni sotto copertura*, cit., p. 442 (rilevando come questa impostazione generi sperequazioni e trascuri le esigenze di tutela dell'indagato rispetto all'abuso investigativo), M. BIRAL, *La testimonianza anonima*, cit., p. 178.

[44] Cass. pen., sez. VI, sent. 9 febbraio 2022 n. 27160, in *C.E.D. Cass.*, n. 283467: «in tema di operazioni sotto copertura, l'inosservanza degli obblighi comunicativi nei confronti del pubblico ministero e la mancanza delle specifiche autorizzazioni previste dall'art. 9 l. 16 marzo 2006 n. 146 non determinano l'inutilizzabilità in giudizio dei risultati dell'attività investigativa svolta dall'agente infiltrato, non potendosi ipotizzare patologie invalidanti degli atti processuali non previste dalla legge e non concretando lo svolgimento di attività di indagine prima che ne sia data notizia al pubblico ministero alcuna lesione di diritti fondamentali traducentesi nella violazione dell'art. 6 Cedu».

[45] L. LUDOVICI, *L'agente sotto copertura*, cit., p. 801.

anche l'attendibilità delle prove reperite e il rispetto delle garanzie difensive[46].

Più convincente, allora, l'opinione di chi – senza scomodare categorie incerte, ma mantenendosi nello stesso quadro concettuale – ravvisa nella normativa sulle operazioni *undercover* un divieto probatorio *ex* art. 191 c.p.p. di tipo "indiretto". Invero, all'art. 9 l. n. 146/2006 e alle altre previsioni che regolano lo strumento possiamo riconoscere natura di norme (anche) processuali: esse attribuiscono un potere investigativo del quale prevedono casi e modi di esercizio.

Sebbene infatti queste previsioni normative siano formulate nei termini di un *esonero di responsabilità penale* degli operanti per attività investigative corrispondenti a condotte di reato allo stesso tempo esse, nel perimetrare l'area della immunità, selezionano i procedimenti in seno ai quali la tecnica d'indagine è consentita, i reati scriminati, le qualifiche soggettive necessarie, le comunicazioni dovute all'autorità giudiziaria (la necessità di un provvedimento, in materia di contrasto alla pedopornografia), in una logica non solo sostanziale (di meritevolezza della pena) ma anche processuale: esse insomma assicurano proporzionalità e sussidiarietà della metodica, bilanciando l'insidiosità del mezzo e le esigenze della repressione penale. Potremmo dire, in sintesi, che il legislatore ha pensato all'immunità penale come a uno *strumento investigativo*.

Siccome le operazioni in parola sono «attività autoritative regolamentate»[47] inidonee a «trovare alcuno spazio di legittimazione al di fuori dei limiti, di materia e procedurali, espressamente previsti», il mancato rispetto della disciplina di legge determina una situazione di "carenza di potere" che giustifica l'inefficacia dell'atto, ossia la sua inutilizzabilità processuale[48]. Un divieto probatorio 'indiretto', insomma[49].

---

[46] M. DANIELE, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen.*, 2013, p. 367 ss.

[47] A. VALLINI, *Il "caso Teixeira de Castro" davanti alla Corte europea dei diritti dell'uomo e il ruolo sistematico delle ipotesi "legali" di infiltrazione poliziesca*, in *Leg. pen.*, 1999, p. 203.

[48] In tal senso C. BORTOLIN, *Operazioni sotto copertura e 'giusto processo'*, in A. BALSAMO, R.E. KOSTORIS (a cura di), *Giurisprudenza europea e processo penale italiano*, Torino, 2008, p. 416; N. GALANTINI, *L'inutilizzabilità effettiva della prova tra*

Questa soluzione richiede di prendere partito sulla questione relativa alla nozione di "divieto probatorio" ai sensi dell'art. 191 c.p.p. Se la sanzione generale dell'inutilizzabilità *ex* art. 191 c.p.p. colpisce solo le prove vietate e non anche quelle acquisite in modo difforme dalle prescrizioni legali[50], dobbiamo concludere che la violazione delle regole acquisitive di una prova in sé ammissibile dà luogo a mere irregolarità, salvo che il *quomodo* probatorio non sia presidiato da una speciale sanzione (nullità, inutilizzabilità)[51]. È certo astrattamente possibile ritenere che esprima una valutazione di inammissibilità, e dunque contenga un

tassatività e proporzionalità, in *Diritto penale contemporaneo - Rivista trimestrale*, 2019, 4, p. 65; F. ZACCHÈ, *Operazioni antidroga sotto copertura condotta dalla polizia municipale*, in *Cass. pen.*, 2013, p. 3576; C. DI BUGNO, *Commento all'art. 14 l. 3 agosto 1998, n. 269 (norme anti-pedofilia)*, in *Leg. pen.*, 1999, p. 164; P.P. PAULESU, *Notizia di reato e scenari investigativi complessi: contrasto alla criminalità organizzata, operazioni «sotto copertura», captazione di dati digitali*, in *Riv. dir. process.*, 2010, p. 800; ID., *Operazioni sotto copertura e ordine europeo d'indagine penale*, in *Archivio penale*, 2018, 1, p. 36; L. PAOLONI, *La controversa linea di confine*, cit., p. 1909 ss. nonché, dello scrivente, *Le indagini* undercover *nel mondo digitale*, in *Penale Diritto e Procedura* (rivista web), 19 ottobre 2023 (ultimo accesso il 28 febbraio 2025); B. PIATTOLI, *Agenti provocatori, indagini "undercover" e diritto alla prova tra limiti di utilizzabilità interni e profili di internazionalizzazione*, in *Dir. pen. proc.*, 2013, p. 565 ss.

[49] M. NOBILI, *La nuova procedura penale, Lezioni agli studenti*, Bologna, 1989, p. 150: «permettere un atto soltanto se (e il soltanto se lo si può ricavare anche in via interpretativa) equivale a stabilire che, al di fuori di quelle ipotesi, sussiste il divieto».

[50] L'inutilizzabilità consegue «alla violazione di quelle regole probatorie dettate allo scopo di impedire che un dato elemento di prova compaia tra le premesse fattuali della decisione» (A. SCELLA, *Inutilizzabilità della prova (dir. proc. pen.)*, in *Enc. Dir.*, Annali, vol. II, tomo I, Milano, 2008, p. 484), perché la formazione della prova presuppone, un «potere istruttorio» e «dove il potere non c'è, perché la legge non lo accorda, l'atto non può non riuscire inefficace» (F. CORDERO, *Procedura penale*, cit., p. 492).

[51] Sarebbe insensato rinvenire un divieto indiretto in ogni disposizione riguardante i *modi* della attività istruttoria: «persino l'inosservanza della regola secondo cui al di fuori dei casi d'urgenza, le operazioni di perquisizione non possono avere inizio «prima delle ore sette e dopo le ore venti» (art. 251, co. 1 c.p.p.) potrebbe essere considerato alla stregua di un motivo di inutilizzabilità del relativo verbale» (A. SCELLA, *Prove penali e inutilizzabilità*, cit., p. 155 ss., che sulla scia di F. CORDERO, *Le situazioni soggettive nel processo penale*, Torino, 1955, p. 156, nota come non sia affatto scontato che il legislatore, pronunciando un dato enunciato normativo, abbia voluto, sia pur implicitamente, pronunciare la derivazione logica dell'enunciato normativo opposto).

'divieto', la norma che subordina il compimento di una attività a uno o più presupposti[52], e sarebbe astrattamente possibile nel nostro caso, ricomprendere nell'*an* i requisiti soggettivi dell'agente *undercover*, i reati per il cui accertamento è consentita l'infiltrazione mascherata, le condotte simulate ammesse, il previo provvedimento giudiziario nella sotto-fattispecie *ex* art. 14 l. 269/1998. In relazione ad altri requisiti diventa però davvero difficile distinguere, ai fini che qui interessano, tra l'*an* e il *quomodo* della prova, se non impiegando l'incerto criterio dell'interesse tutelato dalla previsione[53].

In questo senso, per esempio, è stato sostenuto che l'inutilizzabilità delle informazioni raccolte attraverso un'operazione trasmodata in un *police encitement* rappresenti la conseguenza (non dell'illiceità dell'attività investigativa, né di una regola di esclusione probatoria di matrice convenzionale, ma) dell'inosservanza di un *presupposto finalistico* fissato dalla legge: essa infatti autorizza l'operazione sotto copertura «al solo fine di acquisire elementi di prova» in ordine a certi reati[54].

L'impostazione presenta l'inconveniente di negare, nella materia in questione, la configurabilità di un atto 'irregolare'. Questa difficoltà di distinguere sembra, al fondo, la vera ragione che ha condotto la giurisprudenza a escludere che la comunicazione dovuta al pubblico mini-

[52] Così in relazione alle operazioni relativa al contrasto dei reati contro la libertà sessuale dei minori, *ex plurimis*, Cass., sez. III, sent. 28 gennaio 2005 n. 13500, Spora, in *C.E.D. Cass.*, n. 231605.

[53] Alla proposta di individuare i divieti in base all'interesse, processuale o extraprocessuale, tutelato (N. GALANTINI, *L'inutilizzabilità*, p. 139 ss.), si obietta che quasi ogni norma in tema di prova tuteli un interesse processuale o extraprocessuale, e che è complicato anche individuare quale sia l'interesse, visto che una previsione può soddisfarne più d'uno (A. SCELLA, *Prove penali e inutilizzabilità*, cit., p. 157). Analoga incertezza è rimproverata alla proposta (F.M. GRIFANTINI, *Precisazioni in tema di inutilizzabilità probatoria suggerite da un singolare caso di 'utilizzabilità sopravvenuta' della testimonianza e da una sospetta irritualità della perizia*, in *Cass. pen.*, 1995, p. 3028 ss.) di discernere tra irregolarità e inutilizzabilità connessa al *quomodo* probatorio selezionando all'interno della fattispecie legale, le modalità afferenti al 'nucleo primario', data la vaghezza di tale ultimo criterio (G. GAROFALO, *Divieti probatori e giudizio abbreviato*, in *Ind. pen.*, 2020, p. 158).

[54] Cfr. F. ZACCHÈ, *Operazione antidroga sotto copertura*, cit., p. 3576; L. PAOLONI, *La controversa linea di confine*, cit., 1914; ritiene convincente la conclusione M. BIRAL, *La testimonianza anonima*, cit., p. 177.

stero *ex* art. 9 l. 146/2006, possa avere risvolti sanzionatori[55]: al di là degli argomenti discutibili spesi dalla Corte di Cassazione, l'adempimento in parola risponde a interessi – l'armonizzazione dell'operazione coperta con la strategia investigativa complessiva – che potrebbero risultare eccessivamente tutelati attraverso una sanzione probatoria.

L'alternativa a tutte le ricostruzioni descritte è negare qualsiasi rilevanza processuale alle violazioni, ritenendo che la disciplina delle operazioni coperte sia diretta soltanto a tracciare i confini dell'area della non punibilità, non a limitare l'utilizzabilità processuale degli esiti, cosicché il rispetto delle norme relative ai limiti di liceità delle operazioni sotto copertura rileva solo ai fini dell'eventuale punibilità dell'agente, non dell'utilizzabilità delle prove acquisite né dell'ammissibilità di quelle acquisibili.

Quelle disposizioni, lungi dall'attribuire particolari prerogative investigative alle autorità inquirenti, consentono che le prerogative già riconosciute dalla legge siano esercitate anche in violazione delle norme penali[56]. Accogliendo quest'ultima esegesi, dovremmo concludere, evidentemente, che l'alto rischio di abuso che caratterizza queste meto-

[55] Così (anche se con argomentazioni criticabili, che alludono a prove incostituzionali o anticonvenzionali) Cass. pen., sez. VI, sent. 9 febbraio 2022 n. 27160, in *C.E.D. Cass.*, n. 283467, afferma che «l'inosservanza degli obblighi comunicativi nei confronti del pubblico ministero e la mancanza delle specifiche autorizzazioni previste dall'art. 9 della l. 16 marzo 2006, n. 146 non determinano l'inutilizzabilità in giudizio dei risultati dell'attività investigativa svolta dall'agente infiltrato, non potendosi ipotizzare patologie invalidanti degli atti processuali non previste dalla legge e non concretando lo svolgimento di attività di indagine prima che ne sia data notizia al pubblico ministero alcuna lesione di diritti fondamentali traducentesi nella violazione dell'art. 6 Cedu». Ritiene invece che solo la mancanza della comunicazione al pubblico ministero possa annoverarsi tra le cause di inutilizzabilità, M. BIRAL, *La testimonianza anonima*, cit., p. 169.

[56] In tal senso A. NAPPI, *Nuova guida alla procedura penale on line*, Lanciano (CH), 2020, par. 27.7, nt. 446, il quale ritiene inoltre che l'ammissibilità della prova sia «presupposto, non conseguenza, della liceità dell'operazione sotto copertura: la violazione dell'art. 188, per esempio, renderebbe inutilizzabile la prova e di conseguenza anche illecita la condotta dell'agente sotto copertura». Secondo un'impostazione ancora diversa, L. PARLATO, *Effettività delle indagini ed "equità processuale"*, in A. GAITO, D. CHINNICI (a cura di), *Regole europee e processo penale*, Milano, 2018, p. 137 ritiene inutilizzabili i risultati del *police incitement* e tuttavia ammissibile la prova proveniente dalla deposizione dell'operante *ex* art. 210 c.p.p.

diche investigative venga contenuto dal sistema solo a livello preventivo, attraverso la prospettiva della punizione penale e disciplinare dell'operatore, e trovi una reazione riparatoria alla trasgressione unicamente nella svalutazione normativa dell'apporto dichiarativo dell'agente che abbia trasgredito le prescrizioni legali, per l'applicabilità della regola di valutazione di cui all'art. 192, co. 3 e 4, c.p.p.

Dalla soluzione del quesito sulle conseguenze processuali della violazione della normativa *de qua* discendono poi due ulteriori problemi: quello dell'utilizzabilità delle cose sequestrate nel corso dell'azione sotto copertura abusiva; e quello delle prove acquisite nel corso di azioni sotto copertura legittime, ma relative a reati diversi da quelli per i quali la copertura era stata autorizzata.

Quanto alla questione della rilevanza probatoria delle cose sequestrate nel corso di un'azione *undercover* abusiva, la giurisprudenza della Corte di Cassazione nega che l'illegittimità dell'operazione possa riverberarsi anche sull'eventuale sequestro, così da privare il relativo oggetto di valenza probatoria laddove questo consista nel corpo del reato o in cosa pertinente al reato: in simili casi vale il noto insegnamento delle Sezioni unite secondo cui tra l'attività di ricerca della prova e la sua apprensione non intercorre un vincolo di dipendenza giuridica ma soltanto un rapporto di mera successione cronologica; ciò che è suscettibile di sequestro è tale, infatti, per sue caratteristiche intrinseche normativamente predeterminate – come nel caso di tutto ciò che è pertinente al reato – e non in ragione delle attività attraverso le quali si sia reso possibile il suo ritrovamento, con conseguente impossibilità di propagazione di eventuali vizi da queste a quello[57].

Il secondo problema è quello dell'utilizzabilità delle prove in relazione a reati diversi da quelli per i quali l'operazione sotto copertura è stata disposta e autorizzata: una attività investigativa può sempre offrire modo di acquisire elementi probatori utili (anche o soltanto) per l'ac-

[57] Cass., sez. un., sent. 27 marzo 1996, Sala, in *Cass. pen.*, 1996, p. 3272. La tesi risale a F. CORDERO, *Procedimento probatorio*, in ID., *Tre studi sulle prove penali*, Milano, 1963, p. 122; ID., *Prove illecite, ivi*, p. 158. In argomento, cfr. ID., *Procedura penale*, cit., p. 634 ss.; P. FERRUA, *La prova nel processo penale*, I, *Struttura e procedimento*, Torino, 2017, p. 257 ss.; A. SCELLA, *Prova penale e inutilizzabilità*, cit., p. 178 ss.

certamento di un reato non ricompreso nel catalogo di quelli per i quali essa è consentita.

E proprio nelle operazioni mascherate nel *web* è particolarmente facile che gli operanti si imbattano in delitti diversi e ulteriori rispetto a quello oggetto del procedimento: l'infiltrazione in un gruppo *hacker* o il semplice accesso al c.d. *dark web* può mettere a contatto l'inquirente con condotte illecite inimmaginabili *a priori*, anche molto diverse da quelle in relazione alle quali l'operazione è stata disposta. Stiamo supponendo, evidentemente, che la violazione della normativa su queste operazioni incida sulla spendibilità processuale delle informazioni raccolte.

Nell'esegesi offerta dalla giurisprudenza, la legittimità dell'operazione coperta presuppone la configurabilità, in forza di una valutazione *ex ante* – da collocare, cioè, nel momento in cui è adottato il provvedimento autorizzativo – di uno dei reati inclusi tra quelli legislativamente indicati, non potendo determinare l'inutilizzabilità del materiale acquisito l'accertamento, all'esito delle investigazioni, di un diverso delitto: una diversa conclusione sarebbe in contrasto con l'art. 55 c.p.p. e col principio di obbligatorietà dell'azione penale[58].

In dottrina è stato tuttavia segnalato come l'inutilizzabilità dovrebbe essere riconosciuta almeno in due circostanze: *i*) qualora, già *ab initio*, l'ipotesi di reato originariamente formulata presentava carattere meramente strumentale; *ii*) qualora l'azione *undercover* sia stata portata avanti sebbene l'originaria ipotesi di reato fosse stata ormai messa da parte per manifesta infondatezza e l'unica finalità dell'operazione fosse divenuta ormai quella di acquisire elementi di prova in relazione a reati irrilevanti per l'art. 9 l. n. 146/2006; in questa seconda ipotesi, tuttavia,

[58] La fattispecie potrà verificarsi con qualche complicazione in più nell'ordine europeo di indagine, istituto che considera anche le operazioni mascherate (cfr. d.lgs. 21 giugno 2017 n. 108): cosa accade se l'infiltrazione realizzata per eseguire un ordine emesso dall'autorità italiana per un certo reato conduca alla scoperta di altre fattispecie delittuose non contemplate nell'istanza di collaborazione investigativa? In quel caso potrebbe trovare applicazione l'art. 34 d.lgs. n. 108/2017, che prevede, nell'ambito dello stesso o di altro procedimento, la possibilità di emettere un ordine d'indagine integrativo (P.P. PAULESU, *Operazioni sotto copertura*, cit., p. 27).

la sanzione colpirebbe i soli atti acquisiti nella consapevolezza di operare violando il vincolo di scopo posto dal legislatore[59].

5. Presidi di garanzia

La nostra disciplina, pur non poco complessa, descrive in modo spesso (forse volutamente) vago le attività che è consentito compiere in modo "mascherato". Il dato è spiegabile con la necessaria flessibilità dello strumento, che deve adattarsi alle più disparate esigenze investigative, e tuttavia esso condizione negativamente la capacità regolativa dell'istituto, sia nella perimetrazione della scriminante sia nell'attitudine a orientare la condotta investigativa.

Pesa particolarmente il *deficit* di descrizione legale per indagini 'mascherate' consentite nel *web*: se è innegabile che, oltre una certa misura, la loro tipizzazione sarebbe inopportuna, visto che occorre assicurare alla metodica una certa capacità di adattamento alla continua e velocissima evoluzione delle tecnologie utilizzate per usate per delinquere, appare difficile trarre un qualche 'catalogo legale' di attività, per esempio, dalle previsioni dell'art. 14 co. 2 l. 269/1998 in tema di contrasto alla pedopornografia (si pensi alle identità di copertura utilizzabili per «entrare in contatto con soggetti e siti nelle reti di comunicazione»). Il rischio è che nel mondo digitale l'istituto delle indagini *undercover* favorisca, ancor più che nel mondo fisico, incontrollabili "scorrerie investigative"[60] e, considerata la decisa espansione dell'ambito applicativo delle operazioni *undercover* digitali, il profilo di criticità è tutt'altro che trascurabile, e necessario un maggior sforzo di tipizzazione.

Altro antidoto all'insidiosità di questa metodica investigativa risiede nel controllo giudiziario. Va rilevato, in proposito, che la disciplina generale introdotta nel 2006 prevede invece l'iniziativa degli organi di

[59] L. LUDOVICI, *L'agente sotto copertura*, cit., p. 759.

[60] P. TROISI, *Operazioni digitali sotto copertura*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2019, p. 634.

vertice delle forze di polizia con il solo obbligo di *comunicazione*, previamente e *in itinere*[61].

La costante informazione dell'inquirente è importantissima, come dimostra la circostanza che i procedimenti penali passati alle cronache per operazioni mascherate spregiudicate hanno rivelato proprio una carente supervisione del pubblico ministero[62]. E tuttavia, ai fini del controllo giudiziario – che è funzionale, ricordiamolo, ad assicurare il rispetto del principio di proporzionalità – 'comunicare' è poco.

La disciplina di cui all'art. 9 l. 146/2006, che si accontenta della mera informativa, per un verso «non tiene conto del ruolo 'direttivo' che il sistema assegna al pubblico ministero nell'ambito delle indagini preliminari»; per altro verso, si discosta apertamente dalle indicazioni fornite dai giudici di Strasburgo, secondo cui il coinvolgimento dell'autorità giudiziaria nella fase di avvio delle attività simulate rappresenta addirittura la condizione da cui dipende […] la stessa utilizzabilità processuale dei dati reperiti[63].

Attualmente è invece la prassi che si incarica di armonizzare le norme ai canoni convenzionali e al nostro sistema di rapporti tra autorità giudiziaria inquirente e polizia: quando emerge la necessità di una operazione coperta si considera infatti doveroso per la polizia giudiziaria farne proposta al pubblico ministero – al quale spetta il coordinamento delle indagini, compreso il potere di interdire una tale attività – e solo col suo consenso interpellare i competenti organi di vertice della polizia, ai quali spetta disporre le operazioni e individuare le articolazioni competenti; e saranno poi queste ultime a provvedere, prima dell'inizio delle operazioni, alla "comunicazione" prevista dall'art. 9 l. 146/2006[64]. Insomma, l'eventuale iniziativa degli organi di polizia nasce da un pro-

[61] L'accentramento della titolarità agli organi di vertice evidentemente è funzionale a un controllo di legalità interno e ad assicurare il buon coordinamento tra le attività investigative (simulate e no) che si svolgano «nel medesimo contesto territoriale o criminologico» (M. BIRAL, *La testimonianza anonima*, cit., 170).

[62] F. NANNI, *Conoscenze ottenute sotto copertura*, in AA.VV., *Investigazioni e prove transnazionali*, Milano, 2016, p. 161.

[63] P.P. PAULESU, *Operazioni sotto copertura*, cit., p. 37.

[64] Così P. IELO, *L'agente sotto copertura per i reati di corruzione nel quadro delle tecniche speciali di investigazioni attive e passive*, in *Diritto penale contemporaneo* (rivista web), 5 marzo 2019 (ultimo accesso il 28 febbraio 2025).

getto investigativo condiviso con il pubblico ministero titolare delle indagini.

La disciplina normativa è costituzionalmente dubbia anche perché pecca di irragionevolezza, dal momento che, senza motivazioni in grado di giustificare il differente trattamento, quel *vulnus* non è riscontrabile rispetto alle attività *undercover* volte al contrasto della pedopornografia, subordinate vuoi alla «previa autorizzazione dell'autorità giudiziaria» (co. 1), vuoi alla «richiesta dell'autorità giudiziaria, motivata a pena di nullità» (co. 2)[65].

Fondamentale, ad ogni modo, il controllo *a posteriori*, atteso che l'agente provocatore si muove fatalmente ai confini della legalità: questi possono essere netti in sede di pianificazione dell'operazione, e diventare ambigui nella fase esecutiva. Ma come e quando è verificabile il rispetto delle indicazioni normative in materia di azioni coperte?

Secondo la giurisprudenza se il pubblico ministero ritiene che sia nelle regole l'operato dell'agente sotto copertura, non vi è alcuna notizia di reato da iscrivere *ex* art. 335 c.p.p., in assenza del dato di antigiuridicità (si tratta di una esimente, non di una causa di non punibilità). L'autorità giudiziaria inquirente, perciò, dovrebbe valutare autonomamente il comportamento tenuto dall'agente, che godrebbe, nei fatti, di una sorta di «immunità procedimentale»[66]. Con importanti ricadute sul processo: una volta ritenuti superflui gli adempimenti di cui all'art. 335 c.p.p., nel procedimento a carico dei responsabili dei reati «sollecitati», l'agente può essere sentito sia in veste di persona informata sui fatti, sia, in seguito, in qualità di testimone, e non già quale imputato in procedimento connesso, e alle dichiarazioni vanno applicate le regole di valutazione di cui agli artt. 210 e 192 c.p.p.

È stata proposta un'altra soluzione, assai complicata anche se più armoniosa rispetto ai principi del sistema: ritenere ineludibile, già nelle indagini, il vaglio del giudice sulla condotta dell'agente coperto. Il sindacato sull'antigiuridicità della condotta andrebbe sottratto al pubblico ministero, che sarebbe in ogni caso tenuto a procedere agli adempimen-

[65] Cfr. S. CIAMPI, *op. cit.*, p. 738.

[66] P.P. PAULESU, *Notizia di reato e scenari investigativi complessi: contrasto alla criminalità organizzata, operazioni «sotto copertura», captazione di dati digitali*, in *Riv. dir. process.*, 2010, p. 791.

ti di cui all'art. 335 c.p.p. e alla successiva presentazione di una richiesta di archiviazione. Spetterebbe al giudice investito dell'istanza valutare la posizione dell'agente e, segnatamente, la sussistenza del requisito dell'antigiuridicità delle attività: sarebbe un assetto coerente col ruolo di garanzia del giudice per le indagini preliminari, organo di controllo degli atti di parte[67]. Neppure questa soluzione è tuttavia pienamente giustificabile: se il pubblico ministero riceve notizia delle operazioni e ne segue lo svolgimento senza fare obiezioni è perché ritiene legittima la condotta dunque scriminata e non iscrive.

Allora si potrebbe ritenere che il pubblico ministero debba procedere a iscrizione solo laddove abbia dubbi, a monte, sulla correttezza delle attività comunicate. Sembra la soluzione più equilibrata anche perché l'iscrizione automatica frustrerebbe qualsiasi istanza di tutela dell'identità dell'agente infiltrato.

L'inconveniente di questa soluzione è rappresentato dalla circostanza che essa rende l'iscrizione dell'agente sotto copertura un'ipotesi eccezionale, e comporta l'ampliamento dei casi di ricorso alla testimonianza e alle sommarie informazioni testimoniali con le garanzie di anonimato. E allora si fa più evidente la necessità di perfezionare la disciplina consentendo al giudice di accedere alle effettive generalità del dichiarante e di verificare, di volta in volta, l'assoluta necessità di *preservare l'anonimato*, così da ridurre al minimo indispensabile l'impiego della *testimonianza anonima*.

6. Il d.l. 10 agosto 2023 n. 105: un Covert Cyber Operation Act*?*

Il legislatore attuale sembra non avvertire le criticità fin qui descritte. Lo dimostra il più recente intervento normativo in materia il quale, lungi da qualsiasi intento di sistemazione o di chiarimento sulle metodiche *undercover* e le loro incerte ricadute processuali, si insinua in un provvedimento d'urgenza, per giunta strutturato nel modo disordinato e composito dei 'pacchetti-sicurezza'.

[67] P.P. PAULESU, *ibidem*

Si tratta dell'art. 2-*bis* comma 4 d.l. 10 agosto 2023 n. 105, convertito con l. 9 ottobre 2023 n. 137[68]. Sembra inappropriato chiamarlo *Covert cyber operation act*[69], come fanno gli organi di stampa, solo perché valorizza le indagini sotto copertura in ambiente digitale, ritoccandone la disciplina in relazione ai «delitti commessi con finalità di terrorismo o di eversione» ed estendendone il raggio operativo ai «reati informatici commessi ai danni delle infrastrutture critiche informatizzate individuate dalla normativa nazionale e internazionale»[70]. Al di là di un *potenziamento* dell'istituto, nell'ambito di un complessivo rafforzamento del ruolo della Procura nazionale antimafia e antiterrorismo nel contrasto al *cyber crime*[71], non si vedono affinamenti della disciplina delle indagini digitali *undercover*, anzi alcuni aspetti di criticità risultano addirittura acuiti.

La novella amplia i reati scriminati, estendendone il catalogo alle attività di pirateria informatica, o "hackeraggio": gli operatori possono effettuare *hackback*, ossia controattaccare rispetto ad aggressioni hacker (per recuperare dati rubati, bloccare l'attacco in corso, identificare il pirata informatico, distruggerne gli strumenti), e possono commettere un'ampia serie di reati informatici, tra cui la rimozione delle protezioni di un sistema informatico (c.d. *cracking*), il furto di identità digitale (reato punito dall'art. 494 c.p.), la gestione di *botnet*, reti di computer

[68] Cfr. S. CIAMPI, *Legge n. 137/2023,* cit., p. 723. ; A. CISTERNA, *Attività undercover,* cit., p. 46 ss.; W. NOCERINO, *Le nuove norme di prevenzione e contrasto alla criminalità informatica*, in *Penale Diritto e Procedura* (rivista web), 9 novembre 2023 (ultimo accesso il 28 febbraio 2025).

[69] A. MONTI, *Sicurezza e/o democrazia? Le debolezze strutturali nelle norme italiane sulla* cybersecurity, Repubblica on line, 3 novembre 2023.

[70] Ai nostri fini costituiscono "infrastrutture critiche", vista la loro digitalizzazione e dunque la loro specifica vulnerabilità (cfr. d.lgs. 11 aprile 2011, n. 61) gli impianti di produzione, trasmissione e distribuzione di elettricità, gas e petrolio, i sistemi di approvvigionamento e distribuzione di acqua potabile, le infrastrutture di trasporto, come aeroporti, porti, ferrovie e strade, le strutture sanitarie, le strutture di sicurezza pubblica e protezione civile.

[71] Cfr. A. CISTERNA, *Attività undercover*, cit., p. 49 definisce la novella «una sorta di *upgrading* delle funzioni della Procura nazionale»: alla base, la preoccupazione che le organizzazioni criminali eversive orientino verso la rete le proprie attività, per aumentare le capacità pervasive e nascondere più facilmente i patrimoni illegali.

infetti controllati all'insaputa dei proprietari dei dispostivi, la distruzione di dati e informazioni, Nel consentire, poi, l'attivazione di siti civetta o identità digitali fittizie, o assumere il controllo di un dominio e spazio informatico già esistenti, essa peraltro replica un modello investigativo a forte rischio di trasmodare nel *police encitement*[72].

Le nuove norme ampiano anche la platea dei legittimati, abilitando al compimento delle operazioni *undercover* per l'accertamento dei reati eversivi in parola anche gli ufficiali di polizia giudiziaria in servizio presso l'organo del Ministero dell'interno per la sicurezza dei servizi di telecomunicazione di cui all'art. 7-*bis* d.l. n. 144 del 2005, conv. nella l. n. 155 del 2005[73].

In primo luogo, si nota un certo disinteresse legislativo rispetto all'esigenza di tipizzazione delle condotte consentite: le attività autorizzate scontano il solito *deficit* di determinatezza, riconfermando la strategica vaghezza delle indicazioni normative. Difficile comprendere in cosa si sostanzi un «intervento» su sistemi informatici: la genericità dell'espressione rende plausibile includere tra le condotte scriminate anche l'acquisizione occulta, mediante copia e archiviazione di dati, ma questa esegesi esporrebbe la norma a gravi dubbi di ragionevolezza, se la si raffronta alle previsioni normative che regolano gli atti investigativi digitali che tipicamente sono diretti ad acquisire dati da sistemi informatici e che sono circondati da una serie di garanzie a protezione, tra l'altro, della integrità dei dati e della loro affidabilità[74]. Altrettanto arduo dare corpo all'espressione «attività prodromiche o strumentali» rispetto a quelle specificamente autorizzate dalla legge: qui il legislato-

[72] S. CIAMPI, *Legge n. 137/2023*, cit., p. 732.

[73] A. CISTERNA, *Attività undercover*, cit., p. 49. La legittimazione a compiere queste operazioni non si estende ai membri dei servizi di intelligence perché l'art. 23 l. 3 agosto 2007 n. 124 ha privato il personale del DIS e dei servizi del loro precedente *status* di ufficiale o agente di polizia giudiziaria e di pubblica sicurezza, mentre le garanzie funzionali degli addetti ai servizi, di cui alla predetta legge del 2007, non includono la non punibilità per attività che mettono in pericolo la libertà personale e morale dell'individuo (così A. MONTI, *Sicurezza e/o democrazia?*, cit.).

[74] Cfr. S. CIAMPI, *Legge n. 137/2023*, cit., p. 731. In argomento, cfr. S. SIGNORATO, *Le indagini digitali*, cit., p. 205 ss.

re – lo aveva già fatto in passato – semplicemente «rinuncia alla descrizione analitica»[75].

In secondo luogo, la novella scrimina gli agenti che «attiv[i]no identità, anche digitali, domini e spazi informatici, anche attraverso il trattamento di dati personali di terzi, ovvero assum[a]no il controllo […] dell'altrui dominio e spazio informatico», tutte attività che possono condurre a instaurare dialoghi e conversazioni con altri utenti ignari, interferendo con la libertà e la segretezza delle comunicazioni, che l'art. 15 Cost. presidia con una riserva di legge rafforzata e di giurisdizione[76]. Inoltre, come già osservato, proprio questo ricorso a identità simulate e a sostituzioni di persona sul web genera un alto rischio, per le caratteristiche delle relazioni interpersonali nel mondo virtuale, di trasmodare in attività di 'provocazione'.

Ancora: nessun miglioramento in termini di garanzia giurisdizionale. Anche dopo l'ultima novella, basta una preventiva comunicazione al pubblico ministero ed eventualmente al Procuratore Nazionale Antimafia[77]. Al magistrato inquirente spetterà poi di essere «informato senza ritardo […], nel corso dell'operazione, delle modalità e dei soggetti che vi partecipano, nonché dei risultati della stessa».

---

[75] G. AMARELLI, *Le operazioni sotto copertura*, cit., p. 185; ID., *Le operazioni sotto copertura*, in V. MAIELLO (a cura di), *I reati in materia di criminalità organizzata*, Torino, 2015, p. 180; «parole intollerabilmente vaghe», chiosa A. CAMON, *Disegno di legge spazzacorrotti*, cit., p. 6. Le potenzialità espansive della clausola delle «attività prodromiche e strumentali» sono del resto ben testimoniate dalla esegesi giurisprudenziale della formula nel disposto dell'art. 97 d.P.R. n. 309/1990 in materia di stupefacenti, che viene letta come riferibile «non soltanto con riferimento all'acquisto della droga, ma anche in relazione a tutte quelle altre attività connesse, tese comunque all'accertamento dei destinatari e dei successivi ricettori dello stupefacente» (Cass, sez. IV, sent. 29 maggio 2001 n. 33561, in *Cass. pen.*, 2003, p. 2448), sino all'impiego di documenti falsi, auto con targhe contraffatte, armi clandestine (cfr. P. TROISI, *Le investigazioni digitali sotto copertura*, cit., p. 205).

[76] P. TROISI, *Le investigazioni digitali sotto copertura*, cit., p. 336.

[77] Il decreto introduce l'obbligo, per il p.m. responsabile delle indagini, di comunicare al Procuratore nazionale antimafia e antiterrorismo i provvedimenti adottati nell'ambito delle operazioni coperte relative a una serie di reati informatici di cui al neointrodotto co. 4-*bis* dell'art. 371-*bis* c.p.p. (in precedenza una simile comunicazione era dovuta solo per le indagini coperte relative ai reati di cui all'art. 51 co. 3-*bis* c.p.p.).

Come se non bastasse, la novella normativa rischia di assottigliare il confine già esile tra *intelligence* e repressione penale: la legge obbliga i membri del C.S.I.R.T. (acronimo di *Computer Security Incident Response Team*, la struttura dell'Agenzia nazionale per la *cybersecurity* dedicata agli incidenti informatici, tecnici o di origine delittuosa) a condividere con la Procura nazionale antimafia tutte le informazioni di cui vengano a conoscenza durante il monitoraggio tecnico delle reti; dati che fino a oggi venivano comunicati solo all'ufficio del Ministero dell'Interno responsabile della sicurezza e del corretto funzionamento dei servizi di telecomunicazioni.

In tal modo, è stato osservato, il dovere informativo gravante sull'Agenzia «finisce per attribuire alla stessa (sia pur indirettamente) un potere di impulso investigativo», rendendo «in tal modo sempre più concreto il pericolo di una convergenza di ruoli che dovevano essere separati» e, di conseguenza, di una «osmosi» tra la fase preventiva e quella repressiva[78].

Insomma: mentre le operazioni sotto copertura smarriscono progressivamente il carattere di istituto d'eccezione che lo connotava agli esordi, e acquisiscono caratteristiche sempre più intrusive nelle loro declinazioni 'digitali', i presidi di garanzia – in testa a tutti il controllo giurisdizionale e la determinatezza delle fattispecie liceizzate – hanno ancora ampi margini di migliorabilità.

[78] W. NOCERINO, *Le nuove norme di prevenzione*, cit.

INDAGINI PENALI E CRIPTOVALUTE*

Jacopo Della Torre

SOMMARIO: *1. Premessa. 2. L'impiego delle cripto-attività per finalità illecite. 3. La reazione normativa sovranazionale e interna. 4.* Blockchain *e operazioni di contrasto. 5. Il c.d. "follow the crypto": una nuova realtà investigativa… orfana di regole. 6. Il sequestro delle "monete virtuali": premesse e spunti comparati. 6.1. L'incerto panorama italiano. 7. Conclusioni.*

1. Premessa

La diffusione delle cripto-attività[1] – e, più in generale, della "finanza decentralizzata"[2] – rappresenta uno dei fenomeni più rivoluzionari degli

* La presente ricerca si inserisce nell'ambito del progetto, finanziato dall'Unione europea, "PRIN 2022 PNRR: CRYPTOSAFE (*Towards a safe seizure and confiscation of crypto-assets in criminal proceedings*)". Codice progetto P2022HW85A; CUP D53D23022280001.

[1] Le cripto-attività (termine tradotto in lingua inglese con l'espressione «crypto-asset») costituiscono una categoria omnicomprensiva, capace di inglobare in sé qualunque «rappresentazione digitale di un valore o di un diritto che può essere trasferito e memorizzato elettronicamente, utilizzando la tecnologia a registro distribuito o una tecnologia analoga» (art. 3, co. 1, n. 5 del Regolamento 1114/2023/UE, relativo ai mercati delle cripto-attività – c.d. Regolamento MiCA, per una analisi del quale si rimanda a M. NICOTRA, F. SARZANA DI S. IPPOLITO, M. SIMBULA (a cura di), *Il Micar. Guida al regolamento europeo sui mercati delle cripto*, Milano, 2023 e S. CAPACCIOLI, M.T. GIORDANO, Crypto-asset*: Regolamento MiCA e DLT* pilot regime, Milano, 2023). Antecedentemente all'approvazione del MiCAR, le definizioni erano incentrate maggiormente su una tipologia specifica di cripto-attività, ovvero le criptovalute. Tra le numerose definizioni di «virtual currencies», si veda quella elaborata dal FINANCIAL ACTION TASK FORCE (FATF), *Virtual Currencies. Key definitions and potential AML/CFT risks*, 2014. A livello italiano, un esempio era rappresentato dall'art. 1, co. 2, lett. qq del d.lgs. 21 novembre 2007 n. 231, di recente abrogato dal d.lgs. 28 dicembre 2024, n. 303, a mente del quale la valuta virtuale è «la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per

ultimi anni. Sull'onda del successo avuto dal *Bitcoin* dopo la sua creazione nel 2008[3], in breve tempo si è assistito allo sviluppo in questo settore di un mercato globale, fortemente eterogeneo e in continua ascesa, capace di movimentare, ogni giorno, centinaia di miliardi di dollari[4].

Tuttavia, come era stato preconizzato già nell'ambito del movimento di pensiero c.d. *Cypherpunk*, che ha costituito il retroterra culturale

---

l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente». Cfr. anche l'art. 1, co. 1, lett. d del d.lgs. 8 novembre 2021 n. 184, ove si stabilisce che, «agli effetti della legge penale», il concetto di «valuta virtuale» va inteso come «una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente».

[2] La finanza decentralizzata, o DeFi, rappresenta un ecosistema di applicazioni costruite su tecnologie *blockchain*, con l'obiettivo di offrire servizi di natura economica senza l'intermediazione di enti come banche o istituzioni finanziarie tradizionali. Cfr., per più ampie considerazioni, F. ZATTI, *La regolamentazione della finanza decentralizzata tra sfide attuali e prospettive future: un* "primer", in *Rivista trimestrale di diritto dell'economia*, 2024, p. 433 ss.

[3] L'idea del *Bitcoin* è stata presentata al pubblico il 31 ottobre 2008, mediante la pubblicazione di un *white paper* (reperibile a questo link *https://bitcoin.org/bitcoin.pdf*) da parte di un individuo o di un gruppo, identificatosi con lo pseudonimo di "Satoshi Nakamoto". Il momento non è casuale: si tratta del periodo in cui era scoppiata la grande crisi finanziaria globale, dovuta al fallimento di grandi banche americane come la *Lehman Brothers*. La crisi del 2007-2008 è stata vista come la dimostrazione del fallimento della politica finanziaria, basata sugli intermediari bancari tradizionali. Essa ha favorito il lancio di un nuovo mezzo di pagamento digitale, per l'appunto, il *Bitcoin*, pensato per essere "decentralizzato", cioè, scambiato sulla rete *web* senza la necessaria presenza di intermediari, a cui affidare il compito di controllare la validità delle transazioni (e, in particolare, la mancata "doppia spesa" delle somme).

[4] Nel secondo decennio degli anni Duemila, le monete virtuali hanno progressivamente iniziato a diffondersi in tutto il mondo: oggigiorno se ne contano oramai più di 9000 tipologie che hanno una capitalizzazione di migliaia di miliardi di dollari. Per rendersi conto di quanto il fenomeno sia in ascesa basi prendere quale esempio la criptovaluta $TRUMP, lanciata dal Presidente Trump in occasione del suo secondo insediamento, il cui prezzo è cresciuto in pochi giorni del 45.000%, movimentando un mercato di oltre 10 miliardi di dollari (cfr., al riguardo, *https://www.reuters.com/technology/trumps-new-crypto-token-jumps-ahead-his-inauguration-2025-01-20/*).

per la creazione del fenomeno in esame[5], gli *asset* criptati hanno ben presto attirato l'attenzione, non solo dei comuni risparmiatori, degli istituti bancari e delle autorità governative, ma anche della criminalità[6]. È, del resto, oramai dimostrato come i *bad actors* abbiano repentinamente iniziato a sfruttare le potenzialità del nuovo "oro digitale", al fine di incrementare i profitti. Onde rendersi conto di ciò, è sufficiente menzionare il celebre caso *Silk Road*, cioè il primo *darknet market*, lanciato nel 2011 da un *hacker* statunitense, che, sino alla sua chiusura da parte del FBI nel 2013, ha gestito vendite in *Bitcoin* di beni illeciti di ogni tipo, quantificabili in svariati centinaia di milioni di dollari[7].

In questa sede, mi occuperò del complesso rapporto tra giustizia penale e cripto-attività da tre prospettive. In prima battuta, fornirò un quadro di come esse vengano oggi sfruttate per eterogenee finalità illecite (par. 2). In secondo luogo, analizzerò la reazione che, sul piano sovranazionale e interno, è stata finora intrapresa per far fronte a questa problematica (par. 3). La terza parte avrà, invece, un *focus* prettamente processual-penalistico. Da un lato, mi soffermerò sull'importanza che nelle indagini in questione riveste l'impiego da parte delle autorità di *law enforcement* di algoritmi di analisi della *blockchain*[8], al fine di seguire i flussi di transazioni e di de-anonimizzarle (par. 5). Da un altro lato, mi occuperò delle delicate problematiche giuridiche e applicative

[5] Mi riferisco al *The Crypto Anarchist Manifesto*, in *https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html*.

[6] Per un'analisi cronologica del fenomeno, cfr. D. CARLISLE, *The Crypto Launderers. Crime and Cryptocurrencies from the Dark Web to DeFi and Beyond*, Chichester, 2024 e G. SOANA, *The Anti Money Laundering Regulation of Crypto-Assets in Europe*, Milano, 2024, p. 2 ss.

[7] Cfr. D. CARLISLE, *The Crypto Launderers*, cit., p. 3 ss.

[8] La *blockchain* rappresenta l'infrastruttura tecnologica di base del mondo delle cripto-attività. Per un'agevole spiegazione sul punto, cfr. N. FURNEAUX, *Investigating Cryptocurrencies. Understanding, extracting, and analyzing blockchain evidence*, Chichester, 2018, p. 1 ss. e G. SOANA, *The Anti Money Laundering*, cit., p. 29 ss., v. anche *sub* § 4. Tale concetto ha, oramai, diverse definizioni normative, tra cui è sufficiente qui menzionare l'art. 3, co. 1, n. 2 del MiCAR, il quale si riferisce a «un archivio di informazioni in cui sono registrate le operazioni e che è condiviso da una serie di nodi di rete DLT ed è sincronizzato tra di essi, mediante l'utilizzo di un meccanismo di consenso».

che sorgono nel caso in cui si renda necessario sequestrare gli *asset* in esame (par. 6).

La consapevolezza della complessità che caratterizza i procedimenti penali in cui vengono in rilievo cripto-valute costituirà lo spunto per le conclusioni (par. 7), nelle quali avanzerò alcune proposte utili per una migliore regolazione del fenomeno, concernenti tanto il piano interno, quanto quello sovranazionale.

2. L'impiego delle cripto-attività per finalità illecite

Per avere un'idea del ruolo che le cripto-attività rivestono per l'economia criminale è utile esaminare i *report* elaborati in materia dalle numerose società di *blockchain analitics* oramai esistenti[9].

Le stime maggiormente accreditate a questo riguardo sono quelle sviluppate dall'azienda americana *Chainalysis*, la quale produce uno dei *software* privati di tracciamento dei flussi di cripto-attività più utilizzati anche in Italia. Ebbene, secondo le indagini compiute da questa società, dal 2021 in poi la quantità di *crypto-asset* frutto di traffici illeciti avrebbe sempre superato su scala globale i 20 miliardi di dollari. Per la precisione, la somma sarebbe stata nel 2021 di 26,5 miliardi, nel 2022 di 54,3, nel 2023 di 46,1, mentre nel 2024 di 51,3[10]. E se è vero che si tratta di una fetta di transazioni molto più bassa rispetto alla grandezza complessiva del mercato rispetto a quanto accadeva in passato[11], è altrettanto vero che i dati appena riportati sono fortemente sotto-

[9] Tra i quali, v. CHAINALYSIS, *The 2024 Crypto Crime Report*, reperibile in *https://go.chainalysis.com/crypto-crime-2024.html*; ELLIPTIC, *Typologies Report 2024. Preventing Financial Crime in Cryptoassets*, reperibile in *https://www.elliptic.co/resources/elliptic-typologies-report-2024*; TRM, *Global Crypto Policy Review & Outlook 2023/24*, *https://www.trmlabs.com/eoy-policy-report-2023-24*.

[10] I dati sono tratti da CHAINALYSIS, *Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized*, reperibile in *https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/*.

[11] Cfr. D. CARLISLE, *The Crypto Launderers*, cit., p. 195, il quale ricorda che – secondo i dati di *Elliptic* – nel 2012 almeno un terzo di tutte le transazioni *Bitcoin* erano legate ad attività illecite.

stimati[12]. Si afferma un tanto, non solo perché gli stessi escludono i profitti provenienti «from non-crypto-native crime, such as traditional drug trafficking and other crimes in which crypto may be used as a means of payment or laundering»[13], ma anche in ragione del fatto che essi prendono in esame soltanto gli scambi di cui è già riconosciuta la riconducibilità ad attori criminali. Dal che se ne ricava come vi sia una grande "cifra oscura" di flussi illeciti di cripto-attività, non analizzata neppure dai più avanzati *report* del settore.

Un ulteriore aspetto da prendere in considerazione è costituito dal fatto che i dati in materia dimostrano come il problema della criminalità sulle molteplici *blockchain* esistenti abbia natura globale. Se ciò è vero, va detto che, sempre secondo i dati di *Chainalysis*, il flusso di *asset* illeciti si muove, in particolare, verso alcune giurisdizioni, tra cui spiccano: gli Stati Uniti, la Russia, la Cina, ma anche diversi Paesi europei come il Regno Unito e la Francia. Come dimostrano le oramai numerose operazioni di contrasto portate a termine, va riconosciuto come anche l'Italia sia coinvolta massicciamente nel fenomeno. Onde rendersi conto di ciò, è, d'altra parte, sufficiente mettere in luce come da anni la Direzione Investigativa Antimafia rilevi come

> la criminalità organizzata cerchi di acquisire potere e influenza all'interno dei mercati legali guardando alle nuove frontiere di internet, dove poter sviluppare attività di riciclaggio su vasta scala e poter comunicare indisturbatamente[14].

Vi sono, del resto, plurimi esempi concreti di come finanche le mafie (italiane e straniere) stiano sfruttano le cripto-attività nei loro traffici[15].

Detto ciò, va subito precisato che, a differenza di quanto si potrebbe pensare a primo acchito, l'uso criminale delle criptovalute non è limitato a specifiche tipologie di reati, ma copre ormai qualsivoglia genere

[12] Lo rileva giustamente ancora D. CARLISLE, *The Crypto Launderers*, cit., p. 195.

[13] Cfr. CHAINALYSIS, *Illicit Volumes*, cit.

[14] La citazione è tratta dalla *Relazione al Parlamento della DIA*, II semestre 2021, p. 327.

[15] Cfr. A. ANSELMI, Onion routing, *cripto-valute e crimine organizzato*, Pisa, 2019, nonché A. NICASO et al., The Dark-Web Side of Mafias. *Appalti, crypto e cybercrime. Le mafie adesso, più invisibili e potenti*, Milano, 2024.

delittuoso connesso alla trasmissione di un valore monetario[16]. Non a caso, già alla fine del 2021, Europol aveva affermato esplicitamente che «the criminal use of cryptocurrency is no longer primarily confined to cybercrime activities, but now relates to all types of crime»[17].

Da una prospettiva economica, si è già accennato come le cripto-attività abbiano favorito il repentino sviluppo di veri e propri mercati criminali – presenti nel *deep web*[18], ma anche su *social network* come *Telegram*[19] – in cui si vendono droga, armi, materiale pedopornografico, documenti falsi o rubati, fino ad arrivare alla possibilità di assoldare *killer* e a organizzare il traffico di esseri umani.

Se quanto appena detto è vero, va tuttavia osservato come le fattispecie aventi a oggetto cripto-attività si siano comunque evolute in modo profondo nel corso del tempo.

Da un lato, hanno acquisito sempre maggiore rilievo forme di reati come le truffe *online*, i furti di criptovalute e gli attacchi informatici (i c.d. *ransomware*). Si tratta di illeciti che, oltre a poter destabilizzare il mercato legale (si pensi a casi celebri come gli attacchi all'*exchange* "FTX", oppure a *stablecoins* come "Terra Luna", i quali hanno causato perdite su scala globale per miliardi di dollari), costituiscono una minaccia pure per la sicurezza nazionale, essendo dimostrato come essi

[16] Al riguardo, cfr. N. FURNEAUX, *There's No Such Thing as Crypto Crime. An Investigative Handbook*, Chichester, 2025, p. 67 ss.

[17] EUROPOL, *Cryptocurrencies: tracing the evolution of criminal finances*, dicembre 2021, reperibile in *europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances*.

[18] Al riguardo, va detto che le autorità giudiziarie americane ed europee hanno compiuto, nell'ultimo decennio, una lotta senza quartiere ai c.d. *darknet market*, costellata di grandi successi: pensiamo, per esempio, all'eliminazione da parte della polizia tedesca del *darknet market Hydra* nel 2022, che gestiva traffici illeciti per miliardi di dollari o, per quanto concerne l'Italia, al c.d. "Berlusconi *Market*", smantellato nel 2019 dalla Procura di Brescia. Nondimeno, i dati di *Chainalysis* provano come tale fenomeno sia ben lungi da essere sradicato: cfr. CHAINALYSIS, *The 2024 Crypto Crime Report*, cit., p. 90.

[19] Cfr. l'articolo *ONU: Telegram è un hotspot per fronti e riciclaggio di criptovalute*, reperibile in *https://www.binance.com/it/square/post/14555538331489*.

siano spessi sviluppati da gruppi di *hacker* supportati da autorità statali, come la Corea del Nord[20].

Da un altro lato, è oramai assodato che pure varie organizzazioni terroristiche – tra cui l'ISIS e al-Qaeda – abbiano effettivamente cominciato a sfruttare le criptovalute per raccogliere fondi e/o comprare armi[21]. Risale, per esempio, alla fine di dicembre del 2024 la notizia della condanna pronunciata da una giuria americana nei confronti di un uomo di Springfield, per aver spedito oltre 185.000 dollari in *asset* virtuali a membri dell'ISIS[22].

Ma l'esperienza insegna che il punto d'elezione privilegiato che lega vasti traffici criminali alle cripto-attività è costituita dal riciclaggio[23]. Tali beni si rivelano, invero, da questo angolo visuale particolarmente problematici già solo per il fatto che essi consentono di scambiare, pressoché istantaneamente, flussi di valore da una parte all'altra del globo, senza richiedere l'intervento di una banca o di un altro istituto di investimento tradizionale. Il che significa bypassare, in un solo colpo, i principali soggetti su cui si è da sempre sorretto il sistema contro il *mo-*

[20] Si pensi al ruolo rivestito dal noto "Gruppo Lazarus": D. CARLISLE, *The Crypto Launderers*, cit., p. 97 ss.

[21] In argomento, v. A. BURGESS, R. HAMILTON, C. LEUPRECHT, *Terror on the Blockchain: The Emergent Crypto-Crime-Terror Nexus*, in D. GOLDBARSHT, L. DE KOKER (a cura di), *Financial Crime, Law and Governance*, Cham, 2024, pp. 203 ss.; A. LAVORGNA, *Organised Crime Goes Online: Realities and Challenges*, in *Journal of Money Laundering Control*, 2015, p. 153 ss.; G. MILAD, S.M.A. IRWIN, *The use of crypto-currencies in funding violent jihad*, *ivi*, 2016, p. 407 ss.

[22] La notizia si può reperire al seguente link: *https://www.justice.gov/usao-edva/pr/federal-jury-convicts-springfield-man-crypto-financing-scheme-isis*.

[23] Il tema è ampiamente studiato dalla letteratura penalistica italiana. A quest'ultimo proposito, basti ricordare il dibattito concernente la natura giuridica delle criptovalute e, di conseguenza, la possibilità di sussumere le "monete 2.0" in una delle diverse declinazioni dell'oggetto materiale del reato di riciclaggio ai sensi dell'art. 648-*bis* c.p. Cfr., a livello monografico, G.J. SICIGNANO, Bitcoin *e riciclaggio*, Torino, 2019 e G. SOANA, *The Anti Money Laundering*, cit., *passim*. Si vedano pure L. PICOTTI, *Profili penali del* Cyberlaundering*: le nuove tecniche di riciclaggio*, in *Diritto penale contemporaneo - Rivista trimestrale*, 2018, p. 1121 ss.; F. POMES, *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione*, *ivi*, 2019, p. 159 ss.; M. NADDEO, *Nuove frontiere del risparmio,* Bit Coin Exchange *e rischio penale*, in *Dir. pen. proc.*, 2019, p. 101 ss.

ney-laundering, costruito faticosamente a livello internazionale e interno[24]. Senza contare che le criptovalute consentono di ovviare anche ad alcuni dei maggiori inconvenienti che caratterizzano il denaro contante, laddove impiegato per questi scopi: quali la sua fisicità e la possibilità di identificare, a certe condizioni, le singole banconote utilizzate.

Va, da ultimo, osservato come i criminali abbiano dimostrato grandi capacità di adattamento al repentino sviluppo del mondo delle cripto-attività. A questo proposito, non va trascurato che se, per lungo tempo, le transazioni illecite di cripto-attività hanno avuto a oggetto soprattutto i *Bitcoin*, oggi la situazione è mutata. I dati, infatti, ci dicono che negli ultimi anni stanno iniziano a essere sempre più sfruttate a questo fine altre tipologie di *asset* virtuali, come le *stablecoins*[25]. Ancora, è degno di nota che vari *report* dimostrano come anche gli ultimi derivati del mondo cripto presentino forti rischi. Il riferimento va: a) ai c.d. *Non Fungible Tokens* (NFT), cioè *token* crittografici non replicabili perché registrati in una *blockchain*, quali opere d'arte, video, foto o audio[26]; b) agli strumenti di finanza decentralizzata[27]; c) al metaverso[28]; d) alle forme integrate di portafogli di criptovalute e mezzi di comunicazione criptata.

---

[24] Come sottolinea G. SOANA, *Obblighi di prevenzione del riciclaggio e criptoattività. Interventi legislativi e opportunità regolamentari*, in *Orizzonti del Diritto Commerciale*, 2022, fascicolo speciale, p. 472, «le criptovalute […] nel bypassare la necessità per gli utenti di avvalersi di intermediari negli scambi di valore digitale, intaccano la premessa fattuale su cui è basata la normativa antiriciclaggio – per scambiare valore *online* è necessario avvalersi di un intermediario – diminuendone fortemente la cogenza concreta».

[25] Si tratta di *asset* il cui valore è legato ad altre valute aventi o meno corso legale, oppure ad altri beni (come l'oro).

[26] Cfr., sul punto, il *report* di ELLIPTIC, *NFTs and Financial Crime*, reperibile in *https://www.elliptic.co/resources/nfts-financial-crime*.

[27] Cfr., al riguardo, l'articolo di CHAINALYSIS, *DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate*, reperibile in *https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/*.

[28] Per una guida in materia, v. il *report* di EUROPOL, *Policing in the metaverse: what law enforcement needs to know*, reperibile in *https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know*.

Si può, in definitiva, ben dire che la galassia delle cripto-attività è, oramai, al centro di uno scontro globale tra *bad actors* e autorità legali. I primi hanno sviluppato strategie sempre più sofisticate per eludere i controlli. I secondi hanno cercato di rispondere alla minaccia, sia attraverso strumenti economici[29], sia di tipo normativo (par. 3) e investigativo (par. 4-6).

3. La reazione normativa sovranazionale e interna

Di fronte a un quadro tanto problematico come quello descritto nel paragrafo precedente, gli ordinamenti sovranazionali e interni non potevano rimanere a lungo inerti. Onde evitare che il settore in esame si dimostrasse attrattivo per i criminali già solo perché caratterizzato da una «latitanza della legge»[30], era, infatti, inevitabile che i legislatori reagissero sul piano normativo, cercando di imbrigliarne la natura deformalizzata.

In particolare, si sono a oggi susseguite tre macrofasi di regolazione del fenomeno[31].

In un primo momento, la strategia cardine su cui si è puntato è stata quella di intercettare i principali punti di contatto in "entrata" e in "uscita" del mercato delle cripto-attività, (ri)modulando e aggiornando in questo senso l'insieme dei presidi antiriciclaggio tradizionali. A tale riguardo, deve osservarsi come un ruolo propulsivo sia stato assunto dalla *Financial Action Task Force* (FAFT), le cui indicazioni hanno rappresentato, sin dal principio, il "modello" seguito dal legislatore eu-

[29] Si pensi alla strategia sviluppata dagli Stati Uniti attraverso l'*Office of Foreign Assets Control* (OFAC) per sanzionare a livello economico le maggiori organizzazioni criminali del settore (*https://ofac.treasury.gov/*). Cfr., al riguardo, l'articolo di CHAINALYSIS, *OFAC and Crypto Crime: Every OFAC Specially Designated National with Identified Cryptocurrency Addresses*, in *https://www.chainalysis.com/blog/ofac-sanctions/*.

[30] Cfr. F. CONSULICH, *Nella* wunderkammer *del legislatore penale contemporaneo: monete virtuali che causano danni reali*, in *Dir. pen. proc.*, 2022, p. 153.

[31] Per uno studio analitico della tematica, cfr. G. SOANA, *The Anti Money Laundering*, cit., p. 69 ss.

ropeo nell'approntare una regolamentazione della materia[32]. In tale contesto, va menzionata la Quinta Direttiva antiriciclaggio (Direttiva 2018/843/UE), la quale ha avuto il pregio obbligare i c.d. *exchanges* (cioè, quegli operatori che svolgono il ruolo di cambiavalute tra denaro FIAT e valute virtuali e/o viceversa) e i c.d. *custodian wallet provider* (ovverosia quegli operatori che custodiscono le chiavi private dei portafogli di criptovalute) a rispettare i classici vincoli imposti agli istituti di credito in materia di antiriciclaggio[33]. In tal modo, si è evidentemente cercato di gettare le basi per ricostruire, pure in questo settore "dematerializzato", quella rete di intermediari finanziari che costituiscono l'ossatura dei presidi *AML*[34].

Nonostante gli sforzi profusi a livello europeo e nazionale, deve darsi conto del fatto che – come era stato preconizzato dalla stessa Direttiva 2018/843/UE[35] – siffatta serie di norme non è stata sufficiente a contenere i rischi criminogeni degli strumenti in esame. Sfruttando la rapida evoluzione che caratterizza il settore delle cripto-attività, i *bad ac-*

[32] *FATF*, *Report "Virtual Currencies Key Definitions and Potential AML/CFT Risks"*, 2014; *FATF*, *Guidance for a Risk-Based Approach to Virtual Currencies*, 2015.

[33] Si tratta di una strategia basata sulla condivisibile intuizione per cui, data la ancora scarsa utilizzabilità nel mondo fisico di tali beni, prima o poi essi saranno portati a scambiarle per denaro avente corso legale, dovendo perciò rivolgersi a tali *service provider*.

[34] Queste fonti sono state prontamente recepite sul versante nazionale. Ciò è avvenuto dapprima con il d.lgs. 25 maggio 2017 n. 90 – che ha individuato tra i soggetti obbligati ai fini antiriciclaggio tutti i prestatori di servizi di conversione di valute virtuali in valute aventi corso forzoso – e, in seguito, con il d.lgs. 4 ottobre 2019 n. 125, di attuazione della Quinta Direttiva antiriciclaggio. Quest'ultimo, in particolare, si è spinto – per una volta – ben oltre il contenuto degli atti sovranazionali: esso non si è limitato, infatti, a modificare nuovamente la definizione di valuta virtuale, ma ha anche lodevolmente esteso gli obblighi in esame, oltreché ai «prestatori di servizi di portafoglio digitale», pure ai «prestatori di servizio all'utilizzo di valute virtuali», intesi come tutti coloro che prestano «servizi di emissione, collocamento, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, negoziazione, intermediazione delle valute».

[35] Cfr., il considerando n. 9, dove si affermava che «l'inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non [avrebbe risolto] completamente il problema dell'anonimato delle operazioni in valuta virtuale».

tors hanno, invero, ben presto sviluppato molteplici strategie volte ad aggirare i presidi di tutela approntati dal legislatore. Le principali minacce a questo riguardo sono costituite, per un verso, dall'implementazione di strumenti sempre più sofisticati volti a offuscare le transazioni e farle apparire "lecite" (si pensi all'impiego di meccanismi come *mixers*[36], "ponti" tra una *blockchain* e l'altra[37], oppure criptovalute incentrate sulla *privacy*)[38] e, per un altro verso, dall'utilizzo di cambiavalute non conformi con gli obblighi *AML*[39].

A fronte di tali problematiche, è stata inaugurata una "seconda era" nell'ambito della disciplina sovranazionale del fenomeno delle cripto-attività, volta – in linea con le nuove indicazioni provenienti dalla *FAFT*[40] – a favorire una più adeguata regolamentazione e protezione del mercato, degli investitori, nonché degli scambi che avvengono al suo interno. Si colloca precisamente in questa direzione la recente approvazione del Regolamento 2023/1114/UE relativo ai mercati delle cripto-attività (c.d. regolamento MICA), la cui finalità è proprio quella

[36] Trattasi di strumenti che consentono agli utenti di oscurare la cronologia delle proprie transazioni, aggregando un certo numero di trasferimenti e quindi mischiando l'origine e la destinazione dei pagamenti effettuati: cfr. D. CARLISLE, *The Crypto Launderers*, cit., p. 39 ss.

[37] V., al riguardo, ELLIPTIC, *The state of cross-chain crime*, reperibile in *https://www.elliptic.co/hubfs/Cross%20Chain%20Report%20exec.pdf*.

[38] Si pensi a *Dash*, *Monero* o *ZCash*, le quali si differenziano dalle criptovalute "tradizionali" (come *Bitcoin*) per non essere trasparenti, cioè liberamente osservabili sulla rete. Esse si basano, infatti, su varie tecnologie pensate proprio per offuscare le transazioni e aumentare così il livello di anonimato dei soggetti coinvolti. Sull'impiego di queste criptovalute da parte dei criminali, v. sempre D. CARLISLE, *The Crypto Launderers*, cit., p. 59 ss. L'*asset* più problematico è *Monero*, il quale, pur non essendo del tutto immune al tracciamento, lo rende estremamente difficoltoso: cfr., sul punto, le interessanti ricerche pubblicate da TRM, *The Rise of Monero: Traceability, Challenges, and Research Review*, reperibili al seguente link: *https://www.trmlabs.com/post/the-rise-of-monero-traceability-challenges-and-research-review*.

[39] Possono, per esempio, essere menzionati gli *exchanges* russi Bizlato, Cryptex e PM2BTC recentemente sanzionati dalle autorità statunitensi (OFAC e FINCEN) come enti «primary money laundering concern».

[40] FATF, *Report to the G20 Finance Ministers and Central Bank Governors*, 2018; FAFT, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 2019.

di introdurre una disciplina volta, tanto a favorire lo sviluppo della finanza digitale nei settori «non ancora coperti da atti legislativi dell'Unione in materia di servizi finanziari»[41], in modo conforme a una concorrenza leale, quanto a proteggere i detentori di *crypto-assets* e a garantire la stabilità del mercato. Siffatti scopi sono concretamente perseguiti attraverso un duplice meccanismo: da un lato, si è imputata agli operatori del settore una dettagliata serie di obblighi, il cui mancato rispetto deve essere prontamente sanzionato dalle autorità competenti; dall'altro, si è prescritta agli Stati membri l'adozione di meccanismi punitivi adeguati a reprimere una serie di violazioni, individuate mediante un puntuale rinvio a specifiche disposizioni regolamentari. Va, al riguardo, rilevato come la normativa europea abbia espressamente autorizzato i singoli Stati a impiegare tanto sanzioni di carattere amministrativo, quanto di natura penale. Da questa prospettiva, il nostro ordinamento, con l'approvazione del d.lgs. 5 settembre 2024 n. 129, si è limitato a introdurre una singola fattispecie delittuosa di abusivismo legato a operazione di cripto-attività, privilegiando, per il resto, almeno sulla carta, la strada dell'illecito amministrativo punitivo.

Il regolamento MICA è stato poi affiancato da un nuovo articolato pacchetto di misure, approvate dalle istituzioni UE tra il 2023 e il 2024, le quali hanno aperto una terza stagione regolatoria del fenomeno *de quo*, volta a meglio intercettare i pericoli specifici determinati dal funzionamento tecnologico degli *asset* basati su registri-distribuiti. Il riferimento va, in prima battuta, al Regolamento (UE) 2023/1113, riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività (c.d. Regolamento *travel-rule*), il quale è stato adottato per garantire che le indicazioni della *FAFT* in tema di estensione della cosiddetta "regola di viaggio" alle cripto-attività (consistente nell'obbligo, per i prestatori di servizio di corredare i trasferimenti di fondi di dati informativi relativi all'ordinante e al beneficiario) venissero applicate in modo uniforme in tutta l'Unione[42]. Per quanto qui rileva, va segnalato che, accanto a questa novità di ordine generale, tale atto spicca, non solo perché ha inteso attribuire determinati obblighi ai ge-

[41] Considerando n. 5 del Regolamento.

[42] In merito a tale atto, cfr. la monografia di G. SOANA, *The Anti Money Laundering*, cit., p. 212 ss.

stori dei c.d. *Bitcoin* ATM (*Automated Teller Machine*) o BTM (*Bitcoin Teller Machine*)[43], dato il loro potenziale uso legato al riciclaggio[44], oppure perché ha esplicitamente invitato l'Autorità bancaria europea a emanare orientamenti che specifichino la possibilità di avvalersi di *software* di *blockchain analysis* ai fini preventivi, nei casi in cui vi sia una transazione a rischio particolarmente alto[45]. L'innovazione principale del provvedimento sta, invero, nel fatto che, modificando in modo significativo l'approccio mantenuto in precedenza, l'Unione ha ricompreso nel suo ambito operativo pure le transazioni tra *service provider* e i *wallet* gestiti in modo autonomo dagli utenti (c.d. *wallet* "auto-ospitati")[46]. Così facendo, si è evidentemente cercato di mitigare, almeno in quota parte, il rischio che portafogli digitali di questo tipo si trasformino in uno strumento utile per aggirare l'insieme dei presidi antiriciclaggio faticosamente (ri)costruiti a livello sovranazionale e interno[47]. Di riflesso, è chiaro come, in tal modo, si sia voluto attribuire un sempre più chiaro ruolo di primi guardiani della legalità del settore ai prestatori professionali di servizio di cripto-attività.

Ed è proprio in quest'ottica che si pone anche il nuovo AML *Package*[48], composto dalla VI Direttiva antiriciclaggio (Dir. 2024/1640/UE),

[43] Art. 2, par. 1 e considerando n. 25.

[44] D. CARLISLE, *The Crypto Launderers*, cit., p. 83 ss.; M. HYMAN, *Bitcoin atm: criminal's laundromat for cleaning money*, in *St. Thomas Law Review*, 2015, p. 296 ss., ai quali si rinvia anche per più ampie considerazioni in merito al funzionamento tecnico di tali strumenti.

[45] Considerando n. 17. Cfr. EBA, *Guidelines on templates for explanations and opinions, and the standardised test for the classification of crypto-assets, under Article 97(1) of Regulation (EU) 2023/1114*, 10 dicembre 2024, nelle quali sono contenute varie *red flags* utili per identificare transazioni di matrice particolarmente sospetta.

[46] Ovverosia quelli in cui il cliente ha il pieno controllo delle chiavi crittografiche private. Cfr. *sub* par. 4.

[47] A ogni modo, rimangono ancora fuori dalla disciplina le transazioni dirette tra persona e persona (c.d. P2P). Nondimeno, in proposito il considerando n. 58 precisa che, visti i potenziali rischi determinati da tali tipologie di transazioni, la Commissione UE sarà tenuta entro il 1º luglio 2026 a valutare la necessità di ulteriori misure specifiche in materia.

[48] Pubblicato sulla G.U. dell'Unione il 19 giugno 2024, e destinato a divenire completamente operativo il 10 luglio 2029. Per una visione d'insieme, v. G. SOANA, *The Anti Money Laundering*, cit., p. 203 ss.

dal Regolamento AMLA (Regolamento 1620/2024/UE) e dal Regolamento antiriciclaggio (il Regolamento 1624/2024/UE, c.d. *single rulebook*). È degno di nota come in particolare quest'ultimo provvedimento contenga svariate previsioni innovative per il settore in esame, tra cui spiccano: a) la scelta di obbligare i prestatori di servizi per le cripto-attività ad applicare misure di adeguata verifica della clientela anche per le operazioni occasionali, che risultano rafforzate sopra la soglia di 1.000 euro di controvalore (art. 19); b) la previsione di ulteriori misure di mitigazione dei rischi in relazioni a operazioni con indirizzi autoospitati (art. 40); c) la scelta di vietare ai prestatori di servizi per le cripto-attività la fornitura e la custodia di conti di cripto-attività anonimi o di conti che consentono l'anonimizzazione o un maggiore offuscamento delle operazioni (es. *wallet* con *mixer* integrati, come il celebre *Wasabi Wallet*)[49], anche attraverso monete incentrate sull'anonimato (art. 79).

Va, da ultimo, segnalato che l'Unione europea non si è fermata però qui, ma nel 2024 ha potenziato il proprio sistema di contrasto alla criminalità nel settore in esame mediante la nuova Direttiva 2024/1260/UE, riguardante il recupero e la confisca dei beni[50]. Sebbene, come ribadiremo in seguito, tale provvedimento non detti, in modo criticabile, una

[49] Per un'analisi del ruolo che tale tipologia di *wallet* ha nei traffici criminali, cfr. ELLIPTIC, *Elliptic Research Shows a Dramatic Increase in the Use of Privacy Wallets to Launder Proceeds of Crime in Cryptoassets*, reperibile in *https://www.elliptic.co/media-center/elliptic-research-privacy-wallets-crime-in-cryptoassets*. Non a caso, la *FinCEN* americana, onde far fronte a tale minaccia, ha proposto di adottare una regolamentazione tesa a «identifies international Convertible Virtual Currency Mixing (CVC mixing) as a class of transactions of primary money laundering concern» (cfr. *FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing*, reperibile in *https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency*).

[50] A commento della quale, v. A. DEL GIUDICE, *La nuova direttiva europea sul sistema di* asset recovery. *Novità, impatti, prospettive*, in *Riv. it. dir. proc. pen.*, 2024, p. 1011 ss.; S. FINOCCHIARO, *La nuova direttiva dell'Unione europea in materia di sequestro e confisca*, in *Sist. pen.*, 2024, 6, p. 105 ss.; A.M. MAUGERI, *La nuova direttiva 2024/1269 per il recupero e la confisca dei beni: un complessivo sforzo di armonizzazione per la lotta al crimine organizzato e all'infiltrazione criminale nell'economia*, in *Sist. pen.*, 30 dicembre 2024.

disciplina ablatoria *ad hoc* per i beni in esame[51], esso presenta perlomeno il pregio di ricomprendere esplicitamente gli stessi nelle procedure regolate. Il che rappresenta comunque un segnale di come il legislatore europeo si sia reso conto del fatto che i *crypto-asset* non possono essere oramai più tralasciati, laddove si vogliano contrastare i profitti illeciti delle organizzazioni criminali e riaffermare, anche in questo settore, la validità della massima per cui "il crimine non deve pagare"[52].

4. Blockchain *e operazioni di contrasto*

Nel paragrafo precedente, si è avuto modo di osservare che, negli ultimi anni, è stata introdotta una rete sempre più fitta di previsioni, volte a facilitare il contrasto ai traffici illeciti sulle molteplici *blockchain* esistenti. Come testimoniato dai dati pubblicati dall'Unità di Informazione Finanziaria presso la Banca d'Italia, questi sforzi regolatori stanno effettivamente producendo non trascurabili risultati positivi. Le nuove regole sono, infatti, riuscite ad aumentare, in modo esponenziale, le segnalazioni per operazioni sospette (SOS) riconducibili a *virtual asset*. Basti, in proposito, pensare che si è passati da appena 732 SOS ricevute nel 2019 a 3.453 nel 2021, sino a superare le 5.000 già nel 2022[53]. Il che, evidentemente, dimostra un miglioramento significativo della capacità preventive e repressive dell'ordinamento.

Se ciò è vero, va, del pari, rilevato come, tanto il MiCAR, quanto la corposa disciplina antiriciclaggio approvati in questo settore, non possano essere considerati dei punti d'arrivo, ma solo i primi passi di un percorso che deve essere necessariamente più ampio e ambizioso. Onde contrastare in modo efficace i traffici illeciti che abbiano a oggetto cripto-attività è, invero, indispensabile focalizzare l'attenzione anche su profili ancora non sufficientemente esplorati, tra cui spicca il piano più

[51] Per condivisibili critiche circa tale lacuna, v. A. DEL GIUDICE, *La nuova direttiva europea*, cit., p. 1022 ss. (v. anche *sub* § 6.1).

[52] Sul quale cfr., per tutti, V. MANES, *L'ultimo imperativo della politica criminale:* nullum crimen sine confiscatione, in *Riv. it. dir. proc. pen.*, 2015, p. 1260.

[53] Cfr. *Newsletter 5-2022* della UIF, reperibile all'indirizzo *https://uif.bancaditalia.it/pubblicazioni/newsletter/2022/newsletter-2022-5/index.html*.

strettamente investigativo e processuale. Al riguardo, va, infatti, osservato che, se – come accennato – per quanto concerne il diritto penale sostanziale e quello amministrativo punitivo sono già stati fatti diversi passi avanti, la situazione risulta molto più critica a livello processual-penalistico. E ciò in quanto, da questo angolo visuale, si assiste, finora, a un preoccupante immobilismo legislativo quasi totale, sia a livello sovranazionale, sia interno. Il che rischia di creare problemi di rilevanza cruciale, dal momento che non sempre le previsioni generali contenute nei codici di rito riescono ad adattarsi alle peculiarità del fenomeno *de quo*, venendosi a determinare aree grigie (se non veri e propri vuoti di tutela), pericolose, sia per il rispetto dei diritti fondamentali degli individui, sia per la "tenuta processuale" delle ipotesi accusatorie.

Al fine di dimostrare tale assunto, è necessario ripercorrere – seppur per sommi capi – lo schema di base che caratterizza gli scambi di cripto-valute. Al riguardo, deve anzitutto ribadirsi che, onde trasferire questi beni, è indispensabile avere un "portafoglio" (cosiddetto *wallet*)[54], cioè uno strumento che contiene le chiavi che consentono a livello tecnico le transazioni. Quest'ultime si basano, più propriamente, su uno schema a "criptografia asimmetrica", richiedendo l'utilizzo contestuale di due diverse tipologie di "chiavi"[55]: una "chiave pubblica", impiegata sia per generare gli indirizzi all'interno dei quali sono ricevuti gli *asset*, sia per crittografare i dati della transazione; e una "chiave privata", la quale ha la funzione di autorizzare la spesa. Per trasferire una somma è sufficiente conoscere l'indirizzo del destinatario e siglare la transazione con la chiave privata, senza per forza rivolgersi a un intermediario. A questo punto, il sistema genera una stringa di dati nei quali è indicata la somma trasmessa e gli indirizzi interessati. Dopodiché, intervengono degli utenti (per il *Bitcoin* chiamati *miners*) che hanno il compito di

[54] Molteplici sono le tipologie di *wallet* esistenti: *Paper wallet*, *Sofware wallet*; *Hosted wallet*; *Self-hosted wallet*; *Hot wallet* e *Cold wallet*. Cfr., per un'ampia analisi sul punto, cfr. N. FURNEAUX, *Investigating Cryptocurrencies*, cit., p. 95 ss.

[55] Sul punto, v. la chiara analisi di G. SOANA, *The Anti Money Laundering*, cit., p. 41 ss.

raccogliere le transazioni in un blocco e di "validarlo"[56], cioè di controllare che i vari passaggi di valore siano coerenti con i precedenti blocchi della catena[57]. Una volta compiuta questa operazione, essi aggiungono il nuovo gruppo di transazioni alle precedenti: ed è proprio da questa prospettiva che si coglie il senso del termine *blockchain*, che rappresenta, per l'appunto, una "catena di blocchi" delle transazioni via via compiute.

Sennonché è importante ricordare che le *blockchain* non sono tutte uguali, ma vengono, tradizionalmente, divise in quattro categorie: pubbliche, private, ibride o federate[58]. Per quanto qui rileva, va ricordato che le principali *blockchain* del settore delle cripto-attività – come quella di *Bitcoin* – rientrano nella prima categoria. Esse sono, più in particolare: a) *immutabili*, senza il consenso della rete (difatti, varie copie della *blockchain* sono contenute nei nodi della rete, il che consente al sistema di essere affidabile, evitando la doppia spesa delle somme); b) *decentralizzate*, atteso che non esiste un'autorità regolatoria centrale che prenda in carico gli scambi, ma esse sono gestite dagli utenti della rete, la quale continua a funzionare finché almeno un nodo è attivo; c) *trasparenti*, nel senso che l'importo, la data, l'indirizzo di invio e l'indirizzo di ricezione di ogni transazione sono liberamente osservabili da chiunque; d) *tracciabili*, poiché si può risalire all'esatta provenienza di ogni trasferimento cristallizzato sul registro; e) *pseudo-anonime*[59], in quanto le transazioni pur fornendo un velo di riservatezza, dal momento che sono identificate solo in forma criptata mediante una sequenza di numeri e lettere (c.d. *transaction hash*) e non mediante i nominativi del

[56] Le modalità di validazione cambiano a seconda del diverso "algoritmo del consenso" su cui si fonda la singola *blockchain* di riferimento: al riguardo, v. N. FURNEAUX, *There's No Such Thing as Crypto Crime*, cit., p. 139 ss.

[57] Cfr., ancora, G. SOANA, *The Anti Money Laundering*, cit., p. 36 ss.

[58] V. R. VERMA, N. DHANDA, *Blockchain types: A characteristic view*, in AA.VV., *Distributed Computing to Blockchain Architecture, Technology, and Applications*, Cambridge, 2023, p. 69 ss.

[59] Circa tale caratteristica, v. A. BALASKAS, V.N.L. FRANQUEIRA, *Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges*, in *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Glasgow (UK), 2018, p. 5; C. RUECKERT, *Cryptocurrencies and fundamental rights*, in *Journal of Cybersecurity*, 2019, p. 3; G. SOANA, *The Anti Money Laundering*, cit., p. 45 ss.

cedente e del cessionario, ben possono, tuttavia, essere de-anonimizzate, mediante l'ausilio di determinate tecniche[60].

Ebbene, è evidente che le notazioni appena compiute producono un duplice ordine di conseguenze sul versante investigativo.

In primo luogo, ciò consente di comprendere come nei procedimenti penali legati alle cripto-attività le tecniche d'indagine tradizionali (pur sempre essenziali) debbano essere necessariamente supportate da metodologie di ricerca della prova aventi carattere tecnologico[61]. L'esperienza insegna, infatti, che l'attività di contrasto alla criminalità che abbia a oggetto *crypto-asset*, oltre ad avere spesso una matrice transazionale, richiede l'impiego incrociato di plurimi atti di indagine digitali. Si allude, in particolare, sia al compimento di attività *under cover* telematiche[62], sia alla raccolta massiva di dati da fonti aperte (c.d. *open source intelligence* – c.d. OSINT)[63] e, in particolare, da *social network* (c.d. SOCMIT)[64], sia, infine, all'utilizzo di metodi variegati di analisi della *blockchain* (c.d. *blockchain analysis*)[65]. Le autorità di *law enforcement* hanno, in-

[60] Per un'aggiornata guida operativa sul punto, cfr. N. FURNEAUX, *There's No Such Thing as Crypto Crime*, cit., p. 239 ss. Come anticipato alla nota n. 38, bisogna ribadire che tale operazione di de-anonimizzazione è, invece, molto più complessa, per alcune *privacy coin* come *Monero*.

[61] Cfr. N. FURNEAUX, *There's No Such Thing as Crypto Crime*, cit., p. 109 ss. Nella letteratura italiana, v. G. COSTABILE, *Le indagini digitali*, in AA.VV., Cyber Forensics *e indagini digitali*, Torino, 2021, p. 128.

[62] Cfr., al riguardo, il contributo di P. BRONZO in questo volume.

[63] Si veda sul punto NATO, *Open Source Intelligence HandBook*, 2001.

[64] Sulla quale, v., *amplius*, D. OMAND, *Social Media Intelligence (SOCMINT)*, in R. DOVER, H. DYLAN, M.S. GOODMAN (a cura di), *The Palgrave Handbook of Security, Risk and Intelligence*, Londra, 2017, p. 355 ss.

[65] In argomento, v., *ex multis*, H. ATLAM et al., *Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions*, in *Electronics*, 2024, p. 1 ss.; D. CARLISLE, *The Crypto Launderers*, cit., p. 63 s.; A. BALASKAS, V.N.L. FRANQUEIRA, *Analytical Tools for Blockchain*, cit., pp. 1-8; ELLIPTIC, *Blockchain Analytics & Analysis*, reperibile in *https://www.elliptic.co/hubfs/Blockchain%20and%20Analytics%20Guide.pdf*; N. FURNEAUX, *There's No Such Thing as Crypto Crime*, p. 125 ss.; S. SALISU, V. FILIPOV, *Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation*, in R.L. WILSON, B. CURRAN (a cura di), *Proceedings of the 18th International Conference on Cyber Warfare and Security*, Reading, 2023, p. 338 ss.; G. SOANA, *The Anti Money Laundering*, cit.,

fatti, ben presto imparato a sfruttare alcune caratteristiche intrinseche dei registri-distribuiti delle principali criptovalute, tra cui, in particolare, il loro essere di norma pubblici e liberamente accessibili[66], per ricostruire tramite tecniche di questo tipo i flussi di cripto-attività illeciti e per de-anonimizzarli. E se è vero che diverse attività possono essere compiute in modo manuale dagli operatori[67], va ricordato che, con il tempo, è nata una vera e propria industria di *software* specializzati, utili per scandagliare il *web* alla ricerca di dati di rilievo e per seguire i flussi di denaro[68]. Siffatto *modus operandi*, tuttavia, induce a riflettere, come vedremo a breve, circa la compatibilità di queste nuove metodologie di indagine con il diritto alla riservatezza e alla tutela dei dati personali, specialmente qualora dette operazioni siano compiute in maniera continuativa e massiva, al fine di ricavare un quadro atomistico della "vita finanziaria" (e non solo) dei singoli bersagli[69].

In secondo luogo, le peculiari caratteristiche della tecnologia della *blockchain* incidono, in modo determinante, anche sulle procedure di sequestro aventi ad oggetto le criptomonete collegate a traffici illeciti[70].

---

p. 224 ss.; C. PELKER ALDEN, C. BROWN, R. TUCKER, *Using Blockchain Analysis from Investigation to Trial*, in *Department of Justice Journal of Federal Law and Practice*, 2021, p. 59 ss.

[66] Come si è accennato, fanno eccezione a queste caratteristiche una serie di criptovalute incentrate sulla *privacy*, come *Dash*, *Monero* o *ZCash*.

[67] Cfr., per numerosi esempi al riguardo, N. FURNEAUX, *Investigating Cryptocurrencies*, cit., p. 175 ss.

[68] Sulla nascita di questa industria, cfr. D. CARLISLE, *The Crypto Launderers*, cit., p. 63 ss.

[69] Cfr. *sub* par. 5.

[70] Per una panoramica operativa delle tecniche da seguire per sequestrare efficacemente le cripto-attività, cfr. N. FURNEAUX, *There's No Such Thing as Crypto Crime*, cit., p. 445 ss., nonché A. OWEN, M. NIZZERO, A. LARKIN, *Seizing Crypto: When Asset Recovery Goes Digital*, reperibile in *https://www.rusi.org/explore-our-research/publications/commentary/seizing-crypto-when-asset-recovery-goes-digital*. Nella letteratura italiana, v. M. ANTINUCCI, D. SCAMPOLI, *Il sequestro e la confisca di bitcoin*, in *Dir. pen. proc.*, 2024, p. 1083; F. CAJANI, *Sequestri di files e Bitcoin: i riflessi della dematerializzazione di beni e valute sulla disciplina penal-processualistica italiana*, *ivi*, 2021, p. 742; P. DAL CHECCO, *Sequestro e confisca: tecnica e procedura*, in S. CARPACCIOLI (a cura di), *Criptoattività, criptovalute e Bitcoin*, Milano, 2021, p. 329; R. LUPO, *Quale sequestro per le criptovalute?*, in *ilCentuaro*, 2020, p. 50.

Al riguardo, fermo l'interesse degli ordinamenti giuridici a imporre vincoli reali di diverso tipo su tali beni[71], va registrato il fatto che l'esecuzione degli stessi determina molteplici complessità, tanto di ordine teorico, quanto pratico. Dalla prima prospettiva, occorre sottolineare come, in realtà, gli *asset* virtuali, in quanto beni immateriali, non possono essere tecnicamente oggetto di un sequestro in quanto tale (se inteso come spossessamento fisico di una *res*), potendosi solamente ottenere un effetto giuridico equivalente[72]. Ma ciò che più rileva è il secondo angolo visuale: mi riferisco, in particolare, al fatto che il fortissimo rischio di dissipazione che caratterizza i beni in esame, i quali possono essere trasferiti altrove in un attimo con un *click*, eludendo alla radice le misure ablatorie dell'autorità, rende indispensabile adottare plurimi accorgimenti, onde assicurarsi che le stesse possano andare a buon fine.

Preso atto di ciò, nei prossimi paragrafi ci si concentrerà separatamente sui problemi che entrambi i temi appena menzionati pongono per l'ordinamento italiano, a causa della menzionata inerzia legislativa che caratterizza il settore delle indagini penali in cui vengano in rilievo cripto-attività.

5. Il c.d. "follow the crypto": una nuova realtà investigativa… orfana di regole

Come si è accennato, gli strumenti automatici di tracciamento rappresentano degli ausili fondamentali per contrastare in modo efficace i reati connessi alle cripto-attività. Non a caso, anche in Italia, vari *software* di analisi della *blockchain* sono oramai in dotazione delle autorità di *law enforcement*, le quali li utilizzano quotidianamente in un'ottica

[71] Idealmente, è possibile disporre un vincolo reale sulle monete virtuali attraverso un sequestro probatorio (e, eventualmente, una successiva confisca), in quanto *corpus delicti*, cioè, prodotto, profitto o prezzo del reato (art. 253, co. 2, c.p.p.). Parimenti, esse possono rappresentare l'oggetto di un sequestro conservativo (art. 316 c.p.p.) o preventivo (art. 321 c.p.p.): cfr. Cass. pen., sez. II, 26 ottobre 2022, n. 44378, in *OneLegale*.

[72] Al pari di quanto avviene nel caso di un sequestro di una pagina *Internet*, infatti, pure l'ablazione dei *bitcoin* non può essere realizzata mediante lo spossessamento fisico della *res*, trattandosi, per l'appunto di beni immateriali.

di *follow the crypto*. Essi vengono, più in particolare, impiegati per ordinare a monte e seguire poi a valle la marea di flussi di scambi di *asset* presenti sui diversi registri-distribuiti. Il più delle volte gli investigatori li impiegano con un obiettivo preciso: quello di riuscire a individuare un prestatore di servizi di cripto-attività, come un *exchange*, a cui rivolgere, poi, un ordine di fornire informazioni circa le generalità dei soggetti coinvolti nelle transazioni, riuscendosi così a de-anonimizzare la catena delle stesse[73]. Nel caso si abbia a che fare, invece, con un *provider* che gestisca direttamente le chiave private dei *wallet* per i propri clienti, il vantaggio sarà ancora maggiore, dal momento che si potranno a questo punto finanche bloccare i fondi di interesse, notificando al medesimo un provvedimento di sequestro.

Se ciò è vero, va osservato che, a differenza di quanto accade in altri ordinamenti[74], il nostro codice di rito non detta alcuna previsione specifica, né con riguardo all'OSINT, né in merito agli *investigative tools* atti a tracciare, in maniera più o meno massiva e continuativa, le cripto-attività.

In forza di una prima lettura, si potrebbe, tuttavia, essere portati a giustificare la mancanza di una regolamentazione specifica sul punto sulla base della circostanza per cui i dati analizzati dagli applicativi in questione risultano perlopiù *open access*. Come si è detto, infatti, la maggior parte delle *blockchain* sono pubbliche, così come i dati connessi alle transazioni sul *web* o nei *social network* ricercati tramite applicativi di OSINT. Posto, dunque, che nessuna aspettativa di *privacy* potrebbe essere invocata a fronte di notizie liberamente e consapevolmente esposte "in bella vista"[75] al pubblico, si potrebbe ritenere insussi-

[73] Si tratta, evidentemente, di dati che i *provider* sono tenuti a raccogliere proprio in forza delle sopra esaminate regole antiriciclaggio, approvate negli ultimi anni a livello sovranazionale e interno. Dal che se ne desume come i *tools* di analisi della *blockchain* costituiscono l'apparato tecnico chiave per consentire di sfruttare al meglio la capacità preventiva e repressiva degli obblighi di adeguata verifica della clientela, posti dalla disciplina *AML*.

[74] Cfr. B.J. KOOPS, *Police Investigations in Internet Open Sources: Procedural-Law Issues*, in *Computer Law & Security Review*, 2013, p. 654 ss.

[75] Cfr. B.J. KOOPS, *Police Investigations*, cit., p. 654 ss. Come sottolinea, benché in una più ampia prospettiva, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 166, non «sembrano profilarsi questioni di

stente un obbligo del legislatore di regolare in modo dettagliato i casi e i modi di un loro utilizzo, onde rendere proporzionata l'intrusione nella sfera giuridica del singolo. Ove stessero così le cose, la polizia giudiziaria ben potrebbe avvalersi in autonomia di tali applicativi, in forza dei propri poteri investigativi riconosciuti dalle previsioni generali di cui gli artt. 55 e 348 c.p.p., non essendo, invece, tenuta a richiedere alcun provvedimento autorizzativo emesso da un giudice o dal pubblico ministero.

È opportuno rilevare come un'interpretazione analoga a questa sia stata effettivamente avallata da una delle prima sentenze che, nel panorama mondiale, si è confrontata con simili problematiche. Il riferimento va al caso *Stati Uniti c. Gratkowski*[76], nel quale un imputato aveva chiesto di escludere degli elementi di prova raccolti dagli investigatori grazie all'impiego di uno strumento di analisi della *blockchain* di *Bitcoin*, in forza del rilievo per cui tale attività sarebbe stata compiuta in violazione del suo diritto alla riservatezza, protetto dal IV Emendamento della Costituzione USA. Ebbene, è degno di nota come la *Court of Appeal* per il Quinto Circuito statunitense abbia rigettato tale censura, valorizzando proprio la natura pubblica e liberamente accessibile dei dati contenuti in tale registro-distribuito. Più in particolare, secondo tale pronuncia, poiché la "catena di blocchi" risulta «transparent by design», sarebbe categoricamente da escludersi ogni possibile rilevanza del diritto alla riservatezza con riguardo agli stessi, con la conseguente piena utilizzabilità del materiale ivi raccolto.

Nonostante la presenza di questo precedente, siffatta lettura non convince, per più ordini di ragioni.

In prima battuta, perché essa pare affetta da un significativo vizio logico. Ci si riferisce al fatto che tale esegesi ricava dalla natura *open ac-*

compatibilità con l'art. 8 Cedu […] nel momento in cui un soggetto immette dati in un luogo della rete pubblico o aperto al pubblico». Egli, infatti, «accetta il rischio che quei dati possano essere visualizzati e appresi ovunque, da chiunque, e per qualunque fine. Quindi anche per finalità investigative».

[76] Il riferimento va a *United States c. Gratkowski*, 964 F.3d 307, 312-13 (5th Cir. 2020). A commento della pronuncia, v. D. PENN, *The Fifth Circuit, The Fourth Amendment, and the Third-Party Doctrine: Two Takeaways from the Court's First Ruling on Bitcoin Priv Privacy*, in *Science and Technology Law Review*, 2021, p. 125 ss.

cess di molte *blockchain* una sorta di rinuncia implicita dell'individuo alla riservatezza delle transazioni che lo riguardino. Ma le cose non stanno così: se è, infatti, vero che vari registri-distribuiti sono pubblici, è altrettanto indiscutibile che, come abbiamo ricordato, gli scambi ivi cristallizzati appaiono in modalità criptata, sotto forma di sequenza alfanumerica non riconoscibile, proprio per salvaguardare la *privacy* dei singoli utenti. Che poi gli investigatori, incrociando tali dati con varie tipologie di informazioni rinvenibili o meno *online*, possano riuscire a de-anonimizzare i passaggi di *asset* virtuali è un elemento che, a nostro avviso, non elimina affatto l'aspettativa di riservatezza di base che, comunque, il singolo ragionevolmente continua a mantenere circa il contenuto dei flussi che lo riguardano. Un'aspettativa che si fonda sul fatto che, per la collettività, ogni passaggio di valore presente sulle *blockchain* appare in forma tale da non essere decodificabile, se non con la collaborazione dell'utente o a patto di impiegare mezzi particolarmente intrusivi. Non è, del resto, un caso che, esattamente sulla base di queste ragioni, una parte della giurisprudenza italiana abbia individuato nell'impiego delle cripto-attività una via per occultare all'autorità dei valori, visto il grado di anonimato dalle stesse garantito[77]. Insomma, proprio perché non bisogna fare confusione tra forma della transazione (che può anche essere pubblica) e oggetto della stessa (riservata, perché sotto forma di codice *hash*), che si può ben sostenere che la persona conservi una ragionevole aspettativa di *privacy* con riguardo al contenuto dei dati reperibili sulle *blockchain*[78].

In secondo luogo, va osservato che, come sostenuto da attenta dottrina, l'attività di monitoraggio massivo e di stoccaggio tramite *software* dei flussi di cripto di un individuo, a differenza di un'acquisizione "manuale" *una tantum*, determina, comunque, un'ingerenza di non tra-

[77] Cfr., per esempio, Cass. pen., sez. II, 7 luglio 2022, n. 27023, in *OneLegale*, in materia di autoriciclaggio.

[78] Da questa prospettiva non sembra, infatti, che si possa slegare il momento della raccolta dei dati presenti sulle *blockchain* dal complesso delle operazioni compiute dagli investigatori, le quali sono nel loro insieme finalizzate a de-anonimizzare le transazioni e, quindi, a squarciare il velo di riservatezza assicurato dalle stesse.

scurabile gravità nella sfera riservata dell'individuo[79]. E ciò perché, attraverso il complesso di queste operazioni, l'autorità è messa nelle condizioni di ricostruire una porzione tale della "vita economica" del bersaglio, da poter trarre poi conclusioni precise, o addirittura molto precise, su vari aspetti della sua vita privata, come le abitudini quotidiane, le attività esercitate, le relazioni intrattenute, e così via.

Per quanto concerne il diritto dell'Unione europea, non va poi trascurato il fatto che, tanto l'art. 3 Direttiva 2016/680/UE, quando l'art. 4 del Regolamento GDPR, fanno rientrare nel novero dei *personal data* tutti quelli che sono in grado di rendere identificabile un utente. E non è difficile rendersi conto che i dati presenti nelle *blockchain* pubbliche rientrino in tale categoria proprio perché permettono di risalire, indirettamente, alle generalità degli interessati[80]. Stando così le cose, l'impiego dei *software* in esame, dando vita a un trattamento automatizzato di dati personali, finalizzato ad analizzare la situazione economica e il comportamento di una o più persone, pare rientrare, più in particolare, nel novero delle c.d. "profilazioni", dovendo, pertanto, sottostare al relativo *acquis* eurounitario in materia[81].

---

[79] Cfr., a questo riguardo, le condivisibili affermazioni di C. RUECKERT, *Cryptocurrencies and fundamental rights*, cit., p. 6, secondo il quale «the mere browsing of and searching for data in the blockchain (e.g. with tools like blockchain.info) is not deemed an interference in the right to protection of personal data. However, an intervention in the right to protection of personal data is conceivable, when law enforcement agencies, prosecutors and/or regulators systematically collect, store and/or process data from the blockchain».

[80] V., ancora, C. RUECKERT, *Cryptocurrencies and fundamental rights*, cit., p. 7.

[81] Cfr., al riguardo, A. LYLE, *Legal considerations for using open source intelligence in the context of cybercrime and cyberterrorism*, in B. AKHGAR, P.S. BAYERL, F. SAMPSON (a cura di), *Open Source Intelligence Investigation: From Strategy to Implementation*, Londra, 2016, p. 277 ss.; A. SHERE, *Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis*, in *The New Collection*, 2020, 3, p. 1 ss.; G. SOANA, *The Anti Money Laundering Regulation of Crypto-Assets in Europe*, cit., p. 241 ss. Al riguardo, deve, tuttavia, evidenziarsi una certa contraddittorietà tra la normativa europea in tema di *data protecion* – che mira a rafforzare la tutela della riservatezza in ogni suo aspetto – e le norme in materia *AML*, le quali, all'opposto, sono volte ad agevolare intrusioni nella sfera privata per finalità di contrasto alla criminalità economica.

Da ultimo, la tesi sopra esaminata non convince alla luce di vari orientamenti pretori – strettamente legati – sviluppati in seno alla giurisprudenza della Corte europea dei diritti dell'uomo.

Per un verso, i giudici di Strasburgo hanno, a loro volta, riconosciuto, in tema di indagini penali realizzate sui conti correnti bancari, che la memorizzazione o la raccolta di dati relativi alla situazione finanziaria di un individuo costituisce un'ingerenza nella riservatezza, a prescindere dalla tipologia e dalla natura delle informazioni raccolte[82].

Per altro verso, è degno di nota il fatto che la Corte europea abbia affermato che il concetto di "vita privata", cui si riferisce l'art. 8 Cedu, va inteso in senso ampio, ricomprendendovi anche quelle attività che si svolgono in contesti pubblici[83], come le attività professionali e finanziarie, tra le quali, come si intuisce, ben possono annoverarsi le transazioni monetarie realizzate attraverso la *blockchain*.

Infine, va ricordato che i giudici europei hanno precisato che la mera attività di stoccaggio da parte delle pubbliche autorità «of data relating to the private life of an individual amounts to an interference within the meaning of Article 8»[84], non essendo neppure necessario che le informazioni raccolte vengano poi utilizzate.

Dall'insieme di queste considerazioni, ne consegue una conclusione univoca: l'utilizzo di *sofwtare* di *blockchain analysis* per de-anonimiz-

[82] Cfr. Corte EDU, 1º dicembre 2015, *Brito Ferrinho Bexiga Villa-Nova c. Portogallo*, par. 42 ss.; Corte EDU, 7 luglio 2015, *N. et autres c. San Marino*, par. 51. Cfr., sul punto, G. LASAGNI, *Banking Supervision and Criminal Investigation. Comparing the EU and US experiences*, Cham, 2019, p. 334.

[83] Cfr., benché con riguardo al tema del riconoscimento facciale realizzato in luoghi pubblici, v. Corte EDU, 4 luglio 2023, *Glukhin c. Russia*, par. 64: «the Court reiterates that the concept of "private life" is a broad term not susceptible to exhaustive definition. It can embrace multiple aspects of the person's physical and social identity. It is not limited to an "inner circle" in which the individual may live his or her own personal life without outside interference, but also encompasses the right to lead a "private social life", that is, the possibility of establishing and developing relationships with others and the outside world. It does not exclude activities taking place in a public context. There is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"».

[84] V., per tutte, Corte eur. dir. uomo, sent. 4 dicembre 2008, *S. and Marper c. Regno Unito*, § 67.

zare le transazioni nell'ambito di un'indagine penale, provocano un'ingerenza, che può raggiungere anche un rilievo significativo[85], nel diritto alla vita privata e alla protezione dei dati personali, protetti dall'art. 8 Cedu, nonché dagli artt. 7 e 8 della Carta dir. fond. UE[86]. Non sembra, del resto, un caso che la stessa *FAFT*, pur riconoscendo l'importanza di questi *tools* ai fini *AML*, abbia ricordato che «it is important to consider any potential implications for privacy and data protection in the use of such tools, if they allow transparency that is not otherwise available (e.g. on public blockchains)»[87].

Ne consegue, a cascata, che i legislatori nazionali sono tenuti a rispettare il corrispondente *standard* minimo di garanzie derivante dall'insieme di tali previsioni, il quale è riassumibile nella necessaria presenza di: a) una fonte legale; b) del perseguimento di legittimi scopi di contrasto alla criminalità; e, soprattutto, c) nel rispetto del principio di proporzionalità[88]. E proprio quest'ultimo requisito – inteso nella sua du-

[85] Ciò vale, per esempio, per quei *software* (tra cui anche alcuni tra quelli più utilizzati nel mercato italiano) che cercano di de-anonimizzare le transazioni mischiando, contemporaneamente, le transazioni con altre informazioni *off-chain* sul soggetto, ottenute da fonti come documenti giudiziari, *social media* e più in generale tramite *OSINT*. In tal modo, viene creata una vera e propria rete a strascico di dati, atta a ricostruire la vita privata dell'individuo.

[86] Nello stesso senso, v. anche G. SOANA, *The Anti Money Laundering Regulation of Crypto-Assets in Europe*, cit., p. 244 e C. RUECKERT, *Cryptocurrencies and fundamental rights*, cit., p. 6 s.

[87] FAFT, *Virtual assets and virtual asset service providers*, ottobre 2021, p. 71.

[88] Pertanto, è, a questo proposito, necessario rispettare gli insegnamenti in materia di rapporto tra mezzi di ricerca della prova tecnologici e principio di proporzionalità sviluppati, negli ultimi anni, dalla Corte di giustizia dell'Unione europea. Cfr., tra le molte pronunce sul punto, CGUE, sent. 4 ottobre 2024, causa C-548/21, *Bezirkshauptmannschaft Landeck*; CGUE, sent. 30 aprile 2024, causa C-470/21, *La Quadrature du Net*; CGUE, sent. 7 settembre 2023, causa C-162/22, *Lietuvos Respublikos generalinė prokuratūra*; CGUE, sent. 17 novembre 2022, causa C-432/22, *Spetsializirana prokuratura*; CGUE, sent. 20 settembre 2022, cause C-339/20 e C-397/20, *VD e SR*; CGUE, sent. 20 settembre 2022, cause C-793 e 794/19, *Space Net*; CGUE, sent. 5 aprile 2022, causa C-140/20, *Commissioner of An Garda Síochána e a.*; CGUE, sent. 2 marzo 2021, causa C-746/18 *H.K. c. Prokuratuur*; CGUE, sent. 6 ottobre 2020, causa C-623/17, *Privacy International*; CGUE, sent. 6 ottobre 2020, cause C-511/18, C 512/18 e C-520/18, *La Quadrature du Net*; CGUE, sent. 2 aprile 2018, causa C-207/16, *Ministerio Fiscal*; CGUE, sent. 21 dicembre 2016, cause C-203/15 e C-698/15, *Tele 2 e Watson*;

plice componete di legalità astratta e legalità in concreto – rende inadeguate a soddisfare il livello di garanzie imposto dalla fonte sovraordinata previsioni generali come: a) l'art. 189 c.p.p., in tema di prove atipiche; b) gli artt. 55, 348, o 359 c.p.p., riguardanti le attività investigative delle autorità di *law enforcement*; o, ancora, c) l'art. 234-bis c.p.p., concernente l'acquisizione di documenti e dati informatici[89].

I problemi sollevati dai *tools* in esame non finiscono però qui.

Va, invero, segnalato un problema di "trasparenza algoritmica" che caratterizza alcuni tra gli applicativi più utilizzati nel settore. Ci si rife-

---

CGUE, sent. 8 aprile 2014, cause C-293/12 e C594/12, *Digital Rights Ireland*. Come noto, il punto focale di questa giurisprudenza consiste nel rilievo per cui le ingerenze gravi negli artt. 7 e 8 Carta dir. fond. UE, per essere proporzionate ai sensi dell'art. 52 della medesima Carta di Nizza, devono essere autorizzate da un giudice o da un'autorità amministrativa indipendente, che deve essere in grado di garantire un giusto equilibrio tra i legittimi interessi in gioco. A questo riguardo, la Corte di Lussemburgo ha, del pari, chiarito che la gravità dell'ingerenza nei diritti fondamentali dipende da quanto precise siano le conclusioni rispetto alla vita privata della persona interessata che l'accesso ai dati può determinare. Da ciò ne consegue che, perlomeno nei casi in cui l'impiego dei *software* di *blockchain analysis* finisca, tenuto conto della mole di transazioni analizzate/stoccate e della durata cronologica di controllo su un bersaglio, per produrre l'effetto di consentire di tracciare un quadro analitico della vita finanziaria e dei rapporti sociali di una persona, dovrebbe essere assicurato il medesimo *standard* minimo di garanzie. Per altro verso, un ulteriore punto di riferimento obbligato è costituito dall'art. 20, co. 2, d.lgs. 21 giugno 2017 n. 108, di attuazione della Direttiva 2014/41/UE, relativa all'Ordine europeo di indagine penale (O.E.I.), il quale prevede che all'acquisizione in tempo reale di flussi informatici o telematici provenienti o diretti a banche e istituti finanziari, il procuratore della Repubblica provvede, se necessario, mediante richiesta al g.i.p. secondo quanto previsto dagli artt. 266 e ss. in materia di intercettazioni. Si potrebbe, infatti, ritenere che, data la natura finanziaria dei flussi di transazione di cripto-attività, l'impiego *live* di algoritmi di analisi della *blockchain* per tracciare le stesse nell'ambito di un'indagine penale richieda, per coerenza del sistema, la strutturazione di una disciplina equivalente.

[89] Al riguardo, è utile, infatti, ricordare che nella recente sentenza CGUE, sent. 4 ottobre 2024, causa C-548/21, *Bezirkshauptmannschaft Landeck*, § 99 in materia di sequestro di *device*, la Corte ha stabilito che di fronte a un mezzo di ricerca della prova potenzialmente lesivo degli artt. 7 e 8 della Carta dir. fond. UE, al fine di rispettare l'art. 52 della stessa, il legislatore nazionale è tenuto a «definire in modo sufficientemente preciso gli elementi, in particolare la natura o le categorie dei reati di cui trattasi, da prendere in considerazione». Si tratta, evidentemente, di un requisito non rispettato da nessuna delle disposizioni del codice di rito menzionate nel testo.

risce, in particolare, al fatto che, essendo molti di essi sviluppati da aziende private, le limitazioni derivanti dai diritti di proprietà intellettuale che li caratterizzano non rendono possibile conoscere nel dettaglio le "euristiche" che ne regolano in funzionamento[90]. Il che, come intuibile, incide direttamente, tanto sulla possibilità di valutarne, *cognita causa*, l'affidabilità, quanto di esercitare in modo effettivo il diritto di difesa e al contraddittorio.

Da questa prospettiva, è interessante ricordare la recente decisione adottata dalla *United States District Court* per il distretto della Columbia nel caso *Sterlingov c. USA*[91]. In tale circostanza, l'imputato era accusato di associazione a delinquere finalizzata al riciclaggio di denaro, attraverso la gestione di un noto *mixer* di *Bitcoin*. Per lo svolgimento delle indagini, l'autorità inquirente aveva impiegato uno tra i più importanti *software* privati utilizzati anche in Italia (*Chainalysis Reactor*), che aveva consentito di raggruppare e attribuire al *mixer* tutta una serie di indirizzi, transazioni e prelievi illeciti. Nonostante le censure addotte dalla difesa, volte a mettere in luce l'inaffidabilità dello strumento, definito «unscientific and unreliable» e a escludere, di riflesso, le evidenze così raccolte, la Corte lo ha comunque ritenuto conforme ai criteri di *Daubert* e alla *Federal Rule of Evidence 702*[92].

Se ciò è vero, va osservato come neppure tale decisione sembri costituire un valido "precedente" per gli ordinamenti europei, in generale, e per quello italiano, in particolare. Si afferma un tanto, in ragione della forte valorizzazione che il principio di "trasparenza algoritmica" ha avuto, sia nell'ambito delle Carte sovranazionali volte a dettare i primi principi di fondo dell'applicazione di forme di intelligenza artificiale nell'ambito della giustizia penale[93], sia da una parte della giurispruden-

[90] Il termine "euristica" è impiegato per descrivere le tecniche di raggruppamento (*clustering*) delle criptovalute. Un esempio è l'euristica del *co-spending*: essa assume che più indirizzi su *blockchain* che finanziano una singola transazione siano controllati da un unico soggetto, perché la condivisione di chiavi private tra soggetti diversi è improbabile.

[91] Il riferimento va a *United States District Court, District of Columbia, Sterlingov c. Unites States* (2024), 9 febbraio 2024.

[92] *Sterlingov c. Unites States*, cit.

[93] Il riferimento va, *in primis*, alla Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, 2018, per un commento alla

za interna. È, per esempio, utile ricordare come uno *standard* molto elevato sul punto sia stato fissato dal Consiglio di Stato, il quale ha esplicitamente sostenuto che le esigenze di trasparenza delle forme algoritmiche devono considerarsi prevalenti su quelle di riservatezza delle imprese produttrici dei meccanismi informatici utilizzati[94]. E se tali principi valgono sul piano amministrativo, lo stesso non può accadere – e a maggior ragione – anche in ambito penale, vista la maggiore posta in gioco che caratterizza questo ramo dell'ordinamento.

Ancora, bisogna evidenziare come i *software* in questione, in quanto impiegati per supportare le autorità di contrasto nel valutare «l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati», sembrano rientrare nei meccanismi ad "alto rischio" di cui al combinato disposto tra l'art. 6 e l'allegato III, n. 6, lett. c) del Regolamento 2024/1689/UE[95] (c.d. Regolamento IA). Collocandosi in questa

---

quale, v. S. QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *www.lalegislazionepenale.eu*, 18 dicembre 2018. V. anche l'art. 8 della *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, CM(2024)52-final. Sul piano eurounitario, v. il considerando n. 27 del Regolamento 2024/1689/UE sull'IA, ove si sottolinea l'importanza nel garantire la «trasparenza» dei sistemi algoritmici, ovverosia il fatto che gli stessi siano «sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente i *deployer* delle capacità e dei limiti di tale sistema di IA e le persone interessate dei loro diritti».

[94] Cfr. Cons. Stato, sez. VI, sent. 4 febbraio 2020 n. 881, in *OneLegale*. Sia consentito il rinvio sul punto a J. DELLA TORRE, *Le decisioni algoritmiche all'esame del Consiglio di Stato*, in *Riv. dir. process.*, 2021, p. 713 ss.

[95] I sistemi ad alto rischio sono definiti dal Regolamento come quelli che possono avere «un impatto nocivo significativo sulla salute, la sicurezza e i diritti fondamentali delle persone nell'Unione» (considerando n. 46). Per poter qualificare uno strumento come "ad alto rischio", occorre che siano soddisfatte le condizioni di cui all'art. 6: «a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I; b) il prodotto, il cui componente di sicurezza a norma della lettera a è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell' allegato I» – e di quelli indicati nell'Allegato

prospettiva, dunque, i *tools* di tracciamento dovrebbero essere sviluppati, sin dalla fase di progettazione, in modo che possano essere effettivamente controllati dagli operatori umani nel corso del loro impiego (art. 14, par. 1 del Regolamento IA). L'elaborazione *by design* rappresenta, a ben vedere, una scelta costituzionalmente ed eurounitariamente imposta, giacché solo in tal modo è possibile assicurare l'utilizzo di siffatte strumentazioni in maniera conforme ai diritti fondamentali della persona[96]. Purtroppo, va osservato come, anche da questa prospettiva, i *software* più impiegati in commercio si dimostrano deficitari, a causa del velo di opacità che li caratterizza. Spesso, infatti, non si hanno informazioni sufficienti circa: 1) i tassi di errore che caratterizzano gli algoritmi[97]; 2) il percorso di "allenamento" a cui gli *engine* vengono sottoposti; 3) i presidi volti a evitare possibili effetti discriminatori causati dalla macchina, nonché abusi dei dati personali raccolti; 4) le garanzie specifiche tese a ridurre il rischio che l'IA si comporti come una *black box*, ovvero «sistemi in cui *input* e *output* sono osservabili, mentre il funzionamento interno [del sistema] rimane oscuro persino ai suoi stessi programmatori»[98].

Infine, va rilevato che questi strumenti dovrebbero poter essere utilizzati anche dalla difesa per realizzare un controllo *ex post* sui dati raccolti dall'accusa, oppure per sostenere una propria ipotesi alternativa. Da questa prospettiva, il principio di parità delle parti e il diritto al contraddittorio sembrano, infatti, ostare a un utilizzo degli strumenti in questione in un'ottica unicamente "a carico", spingendo, per converso, per un loro possibile impiego anche in favore del prevenuto. Il che, visti

III. Per una sintesi dei profili processual-penalistici del Regolamento in questione, cfr. S. QUATTROCOLO, *Intelligenza artificiale e processo penale: le novità dell'*AI Act, in *Diritto di difesa*, 16 gennaio 2025; M. TORRE, *Il Regolamento europeo sull'intelligenza artificiale: i profili processuali*, in *Processo penale e giustizia*, 2024, p. 1534 ss.

[96] Cfr., per più ampie considerazioni sul punto, B.J. KOOPS, J.H. HOEPMAN, R. LEENES, *Open-source intelligence and privacy by design*, in *Computer Law & Security Review*, 2013, p. 676 ss.

[97] Proprio un problema di questo tipo era stato denunciato dalla difesa nel già citato caso *Sterlingov c. Unites States*, cit. nei confronti del *software Chainalysis Reactor*.

[98] La citazione è tratta da G. CONTISSA, G. LASAGNI, G. SARTOR, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di internet*, 2019, p. 620.

i costi notevoli che hanno i più avanzati tra questi *software*, richiederebbe che la difesa possa quantomeno ottenere che un proprio consulente sia messo nelle condizioni di utilizzare gli strumenti a disposizione dell'autorità. Nulla di tutto ciò, è, peraltro, previsto, né a livello sovranazionale, né nel codice di rito.

L'insieme di queste considerazioni ci porta a ritenere che, in assenza di una normativa che ne disciplini nel dettaglio i casi e i modi di utilizzo, l'impiego di *software* automatizzati di *blockchain analysis* dovrebbe, a rigore, considerarsi inibito nel nostro ordinamento processuale penale, data la compressione – non adeguatamente bilanciata da un vaglio di proporzionalità in astratto e in concreto – che gli stessi determinano su plurimi diritti fondamentali della persona. Con la conseguenza che dovrebbe essere vietata l'acquisizione dei loro risultati e/o utilizzazione nel procedimento. E ciò, in primo luogo, sulla base del "combinato disposto" tra artt. 189 e 191 c.p.p.: al riguardo, pare, invero, da condividere la tesi di chi ritiene che dall'art. 189 si ricavi un divieto probatorio implicito nei confronti di elementi probatori non disciplinati dalla legge acquisiti in spregio alle garanzie primarie dell'uomo, la cui violazione è causa di inutilizzabilità patologica[99].

Un'interpretazione di questo tipo pare imposta, a maggior ragione, in ragione dei problemi di trasparenza sopra segnalati, i quali impediscono alla difesa di avere un contraddittorio effettivo sull'affidabilità e sul funzionamento di tali strumenti. Come affermato da attenta dottrina, in un'evenienza di questo tipo, infatti, onde salvaguardare i pilastri del *fair trial*, nelle sue articolazioni del contraddittorio e della parità delle armi, è necessario agire a monte direttamente sul piano dell'ammissibilità probatoria, rispetto a quello della valutazione, prevedendo che «the court should exclude the "black box evidence" from the adjudication on the defendant's guilt»[100].

[99] In tal senso, v. C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007, p. 173; P. TONINI, C. CONTI, *Il diritto delle prove penali*, Milano, 2014, p. 105. *Contra*, invece, M. DANIELE, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen.*, 2013, p. 370.

[100] Testualmente, S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020, p. 96, nonché M. GIALUZ, S. QUATTROCOLO, *Predictive justice in Italy*, in *Revue*

Al proposito, non va, infine, tralasciato come, nonostante la nota ritrosia delle istituzioni sovranazionali a imporre regole circa l'ammissibilità e la valutazione delle prove[101], questa conclusione trova supporto anche nella giurisprudenza della Corte di giustizia dell'Unione europea. E ciò in quanto i giudici del Lussemburgo hanno negli ultimi anni messo in rilievo, in un numero via via più ampio di sentenze, la necessità di escludere informazioni ed elementi di prova[102], ottenuti in violazione degli artt. 7, 8, 47 e 48 della Carta di Nizza, laddove vi sia il rischio che l'ammissibilità degli stessi impedisca alla difesa «di svolgere efficacemente le proprie osservazioni in merito a un mezzo di prova rientrante in una materia estranea alla conoscenza dei giudici e idoneo a influire in modo preponderante sulla valutazione dei fatti»[103]. Ebbene, dati i gravi problemi di opacità che affliggono molti *software* di *blockchain analysis*, è difficile negare che si ricorra proprio in una situazione di questo tipo, la quale impone l'esclusione del mezzo di prova al fine di evitare una violazione siffatta.

Se questa soluzione è imposta dal doveroso rispetto delle garanzie della persona, va, tuttavia, ammesso come la stessa non sia affatto a costo zero per l'ordinamento. E ciò, in quanto, come abbiamo avuto modo di osservare, i *tools* in questione sono assolutamente indispensabili per un efficiente contrasto alla criminalità. Alla luce di ciò, non stupisce che, nella prassi, gli investigatori, pur di non privarsi di tali mezzi, siano soliti utilizzare un *escamotage*: essi continuano a impiegarli, ma solo come "spunti investigativi", che vengono poi riscontrati tramite atti di indagine tradizionali, validamente utilizzabili in fase procedimentale e processuale. Non sfuggirà che l'operazione da ultimo descrit-

Internationale de Droit Pénal, 2023, p. 205. V. anche L. LUPÁRIA DONATI, G. FIORELLI, *Diritto probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale*, in *Diritto penale contemporaneo - Rivista trimestrale*, 2022, 2, 43.

[101] Cfr., *amplius*, A. CABIALE, *I limiti alla prova nella procedura penale europea*, Milano, 2019.

[102] Cfr., al riguardo, tra le tante, C. giust., 5 settembre 2024, *M.S.*, C-603/22, par. 172; C. giust., 14 maggio 2024, *Stachev*, C-15/24; Corte giust., 30 aprile 2024, *M.N.*, C.670/22, par. 131; C. giust., 2 marzo 2021, *H.K.*, C-746/18, par. 44; C. giust., 6 ottobre 2020, *La Quadrature du Net e a.*, C-511/18, C-512/18 e C-520/18, par. 226.

[103] La citazione è tratta da C. giust., 6 ottobre 2020, *La Quadrature du Net e a.*, C-511/18, C-512/18 e C-520/18, par. 226.

ta, pur riducendo l'impatto negativo della tecnologia in esame sui diritti fondamentali, fanno comunque pagare ai singoli prevenuti la criticabile inerzia del legislatore in questa materia[104].

6. Il sequestro delle "monete virtuali": premesse e spunti comparati

Come si è avuto modo di anticipare, la struttura decentralizzata della rete *blockchain* assume particolare importanza pure con riguardo alla procedura di ablazione avente ad oggetto le cripto-attività. Infatti, se, con riguardo alla "moneta analogica", gli investigatori possono ricercare e sequestrare documenti e conti bancari con relativa agilità rivolgendosi agli istituti di credito, per quanto concerne gli *asset* digitali in esame, la possibile mancanza di un *service provider* che funga da intermediario e la loro estrema volatilità, rende infruttuose siffatte modalità operative classiche[105].

A fronte di ciò, si comprende la ragione per cui varie organizzazioni internazionali – come il GAFILAT, l'INTERPOL, l'OSCE e il Consiglio d'Europa[106] – abbiano sviluppato *guidelines* specifiche in materia, al fine di supportare le autorità di *law enforcement* nello sviluppo di un'efficace attività tesa all'ablazione reale delle criptomonete legate a operazioni illecite. Proprio in quest'ottica si spiega il perché, nell'ambito del Fondo Monetario Internazionale, si sia finanche affermato che il fenomeno in esame «require adjusting some legal requirements and practices (e.g., freezing/seizing orders to be issued by a court)», onde

[104] Difatti, spesso l'intera catena probatoria e indiziaria trova origine proprio nell'impiego – non regolato – di tali applicativi.

[105] C. RUECKERT, *Cryptocurrencies and fundamental rights*, cit., p. 4.

[106] Cfr., per esempio, COUNCIL OF EUROPE AND EUROPEAN UNION, *Guidelines for the management of seized assets*, 2023; INTERPOL, *Guidelines for the Seizure and Sale of Virtual Assets*; CYBERCRIME PROGRAMME OFFICE OF THE COUNCIL OF EUROPE, *Guide on seizing cryptocurrencies*, 2021; FINANCIAL ACTION TASK FORCE OF LATIN AMERICA, *Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets*, 2021; iPROCEEDS-2, *Guide on seizing cryptocurrencies*, 2021.

consentire di realizzare un'attività di prevenzione e di repressione efficiente[107].

Come abbiamo avuto modo di anticipare, anche l'Unione europea ha cominciato a interessarsi della materia, attraverso l'approvazione della Direttiva 2024/1260/UE. Tale provvedimento, infatti, menziona esplicitamente le cripto-attività tra i beni che possono essere sottoposti a sequestro e confisca nell'ambito di un procedimento penale[108]. Per di più, va segnalato che, proprio perché il legislatore eurounitario, rendendosi conto del grande rischio di dissipazione che concerne tali *asset*, li ha ricompresi tra quelli che dovrebbero poter essere recuperati tramite "azioni immediate" degli Uffici per il recupero dei beni, istituiti per agevolare la cooperazione transfrontaliera in relazione alle indagini per il reperimento dei beni[109]. Se un tanto è vero, va, tuttavia, segnalato che la Direttiva in questione presenta ancora il vistoso limite di non contemplare una procedura ablatoria *ad hoc* per le cripto-attività, andando, dunque, estese alle stesse le fattispecie generali ivi regolate[110]. Dal che ne consegue come gli Stati membri godano ancora di grande discrezionalità nel valutare come adattare le proprie forme di sequestro e confisca al contesto in esame.

Ciò nondimeno, va segnalato che diversi ordinamenti non sono comunque rimasti inerti, ma hanno già adottato linee guida specifiche, se non veri e propri *corpus* normativi organici sul punto.

Dalla prima prospettiva, possono menzionarsi, a mero titolo esemplificativo, le *guidelines* elaborate dal *Ministerio Público Fiscal de la Nación* in Spagna[111] e dalla Procura generale slovena[112], nelle quali so-

[107] Così si esprime, testualmente, il *report* del Fondo Monetario Internazionale, redatto da N. SCHWARZ et al., *Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations*, in *FinTech Notes* No 2021/002.

[108] Considerando n. 12 e art. 3, co. 1, § 1, n. 2.

[109] In Italia, tali uffici già sono istituiti presso il Servizio per la Cooperazione Internazionale di Polizia, strutturalmente incardinato presso il Ministero dell'Interno.

[110] In questo senso, v. anche A. DEL GIUDICE, *La nuova direttiva europea*, cit., p. 1022.

[111] Cfr. MINISTERIO PÚBLICO FISCAL DE LA NACIÓN, *Guía práctica para la identificación, trazabilidad e incautación de criptoactivos. Consideraciones teórico-prácticas*

no stati cristallizzati una serie di principi e buone prassi da seguire nel corso delle procedure ablative aventi ad oggetto valute virtuali[113]. Pur trattandosi di atti non aventi carattere vincolante (*soft law*), essi presentano indubbiamente il pregio di individuare *standard* uniformi applicabili su tutto il territorio nazionale.

Sul secondo versante, merita menzionare, in particolare, la ricca regolamentazione implementata in materia dal Regno Unito. Ci si riferisce alla Sezione 180-Allegato 9 dell'*Economic Crime and Corporate Transparency Act 2023*[114], la quale ha introdotto disposizioni *ad hoc* all'interno del *Proceeds of Crime Act 2002* (POCA), con l'intento di disciplinare analiticamente «searches, seizure and detention of cryproassets»[115]. Si tratta di un provvedimento al quale occorre guardare con vivo interesse, atteso che esso rappresenta uno dei primi tentativi su scala globale di fornire un quadro normativo organico di tale complessa materia.

Il primo dato da prendere in considerazione è che la riforma in esame è intervenuta, tanto sulle misure ablatorie di matrice strettamente penalistica, regolate dalle parti 2, 3 e 4 del POCA, quanto sulle azioni ablatorie di matrice civilistica (o azioni *in rem*), regolate nella parte 5 del POCA, che non richiedono una condanna del prevenuto, attraverso cui è in tale ordinamento possibile ordinare l'immediato spossessamento di beni che si ritiene siano stati ottenuti attraverso una condotta illecita (o destinati a un tale scopo).

---

sobre activos virtuales basados en la tecnología de cadena de bloques y su investigación penal, 2023.

[112] V. STATE PROSECUTOR GENERAL OF THE REPUBLIC OF SLOVENIA, *Decision No. VDT-Tu-15-5/4/2019*.

[113] Cfr., per esempio, INDIANA STATE POLICE, *Seizure of Cryptocurrency and Virtual Currencies*, 2018; CYBERSECURITY MALAYSIA, *Policy and procedure for seizing cryptocurrencies*; REGIONAL ORGANIZED CRIME INFORMATION CENTER, *Bitcoin and Cryptocurrencies: Law Enforcement Investigative Guide*.

[114] Il testo del provvedimento è reperibile al seguente *link*: *https://bills.parliament.uk/bills/3339*.

[115] L'espressione *cryptoasset* è definita come «a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically».

Sul piano penalistico, le modifiche principali apportate sono sostanzialmente tre.

In primo luogo, è stato rimosso il requisito che una persona sia stata arrestata prima di poter utilizzare i poteri di sequestro. Questa modifica si applica a tutti i beni, ma è stata esplicitamente ritenuta particolarmente utile nel contesto dei *crypto-asset*.

In secondo luogo, in conformità alle più avanzate *guidelines* sviluppatesi a livello sovranazionale, sono state introdotte disposizioni atte a modificare i poteri di perquisizione, sequestro e custodia in modo tale da rendere esplicitamente chiaro il potere della autorità di *law enforcement* di "ricreare" portafogli di criptovalute e trasferire i beni in un portafoglio controllato dalle forze dell'ordine (c.d. *Government-controlled wallet*).

In terzo luogo, si è attribuito alle *Magistrates' Court* (come autorità responsabile per l'esecuzione degli ordini di confisca) il potere di autorizzare la vendita di qualsiasi *crypto-asset*, nello stesso modo in cui esse potevano già farlo con i contanti, oppure i fondi detenuti in conti bancari.

Con riguardo alle *civil forfeiture*, è stato introdotto un intero sottoinsieme di poteri ablatori specifici, finalizzati a consentire all'autorità di recuperare le cripto-attività di sospetta origine illecita il più rapidamente possibile. Per quanto qui rileva, l*'Economic Crime and Corporate Transparency Act* 2023, si compone di quattro capitoli, idealmente rappresentativi dei diversi momenti che compongono il complesso iter ablativo.

Il primo (3C) è dedicato alla fase del «seizure and detention of cryptoassets». Si stabilisce, al riguardo, che un *enforcement officer* possa ricercare un qualunque oggetto collegato alle criptovalute – denominato «cryptoasset-related item»[116] – a condizione che vi siano «reasonable grounds» per sospettare che in un determinato luogo si trovino uno o

[116] A tali fini, la locuzione «cryptoasset-related item» è intesa in senso ampio, ossia come qualsiasi bene che contiene o può dare accesso a informazioni potenzialmente utili per un eventuale sequestro. Si pensi, per esempio, a pezzi di carta in cui sono state scritte le *password* per accedere al *wallet*, a varie tipologie di *hardware memory sticks* utilizzate per memorizzare una chiave privata o, ancora, a *smartphone* contenenti applicazione che forniscono all'utente il controllo su un portafoglio di criptovalute.

più beni connessi ad attività illecite. Una volta rinvenute eventuali cripto-attività, l'autorità è legittimata a sequestrarle, laddove vi siano ragionevoli motivi per ritenere che tali *asset* siano di provenienza delittuosa o siano a ciò destinati. Più in particolare, il provvedimento stabilisce, anche in questo caso, che venga operato un trasferimento delle criptomonete «into a crypto wallet controlled by the enforcement officer», al fine di garantire l'effettivo spossessamento della *res*.

Il Capitolo 3D della legge attribuisce poi poteri ulteriori agli ufficiali di polizia, legittimandoli a richiedere un ordine di congelamento («crypto wallet freezing order») delle criptovalute detenute in portafogli crittografici gestiti da un «UK-connected cryptoasset service provider»[117], laddove vi siano ragionevoli motivi per sospettare che ivi siano presenti beni destinati all'uso in condotte illecite[118].

Una volta concluso l'*iter* di spossessamento, il Capitolo 3E, intitolato «forfeiture of cryptoassets following detention or freezing order», consente all'autorità giudiziaria di ordinare la confisca civilistica di alcuni o di tutti i *cripto-asset* detenuti in conformità a un ordine di sequestro (Capitolo 3C) o di congelamento (Capitolo 3D).

L'ultimo passaggio della procedura è disciplinato dal Capitolo 3F, il quale regolamenta la delicata questione relativa alla conversione dei *crypto-assets*. Attesa l'estrema volatilità di tali beni, si stabilisce che l'*enforcement officer* o la persona a cui sono stati sequestrati i criptovalori possano richiedere al tribunale competente di emettere un'ordinanza che imponga la loro conversione in valuta FIAT. A fronte della richiesta, è prevista l'instaurazione di una fase in contraddittorio che coinvolge tutti i soggetti interessati, all'esito della quale il tribunale adotterà la propria decisione basandosi sulla probabilità che i beni (nel

[117] La disposizione prevede che all'interno di tale categoria debbano essere incluse tutte quelle entità che: a) hanno una sede legale nel Regno Unito e le loro attività quotidiane sono svolte da tale ufficio o da un'altra sede nel Regno Unito; b) hanno termini e condizioni con le persone a cui forniscono servizi che prevedono che una controversia legale possa essere dibattuta nei tribunali del Regno Unito; c) conservano nel Regno Unito i dati relativi alle persone a cui forniscono servizi.

[118] Merita di essere sottolineato che la legge non individua una soglia minima per gli ordini di congelamento del portafoglio crittografico.

loro complesso) possano subire una significativa perdita di valore durante il periodo che precede il rilascio o la confisca[119].

6.1. L'incerto panorama italiano

Purtroppo, va rilevato che il panorama italiano risulta molto diverso rispetto a quello appena descritto. Anche a questo proposito il legislatore interno ha, infatti, manifestato un atteggiamento di completa apatia. Né all'interno del codice di rito, né in alcuna legge speciale, è dato rinvenire una disciplina specifica in punto di misure ablatorie che interessino le cripto-attività. Si tratta di una situazione che merita di essere stigmatizzata, specie in ragione del fatto che la procedura volta al sequestro di questa categoria di beni è caratterizzata, come già anticipato, da molteplici rischi, attesa la loro natura immateriale e volatile.

Dal punto di vista teorico, vi è, anzitutto, la necessità di distinguere a seconda della tipologia di *wallet* che si voglia apprendere[120].

Si consideri, in primo luogo, il caso di un *custodian wallet*, con riguardo al quale è necessario effettuare una richiesta di sequestro, eventualmente tramite rogatoria od OEI, a un *service provider* per chiedere e ottenere il congelamento delle somme di denaro. Da questa prospettiva, invero, perlomeno fino a quando non diverrà concretamente operativo il Regolamento *e-evidence*[121], i tempi, spesso dilatati, necessari per ottenere una risposta a un ordine rivolto a un prestatore di servizio di cripto-attività rischiano di risultare del tutto incompatibili con l'estrema rapidità necessaria per sequestrare i beni in esame.

Nell'ipotesi di un portafoglio gestito in autonomia dall'utente (c.d. *self-hosted*) invece, le operazioni sono ancora più complesse. Laddove, la chiave privata sia rappresentata su un bene fisico (si pensi, per esempio, a un foglio di carta o a un diario), è necessario anzitutto rico-

[119] Occorre ricordare come la disciplina in questione sia ispirata dal principio generale per cui la conversione delle valute deve avvenire «in the manner best calculated to maximise the amount of money obtained for the cryptoassets».

[120] Per approfondimenti, v. P. DAL CHECCO, *Sequestro e confisca: tecnica e procedura*, cit., p. 336-340.

[121] Ci si riferisce al Regolamento 2023/1543/UE. In tema di acquisizione transfrontaliera di prove digitali, sul quale cfr. il contributo di R. BELFIORE in questo volume.

noscerla e, in secondo luogo, sequestrarla. Per contro, nel caso in cui essa sia conservata all'interno di un *device* digitale, la sua apprensione presuppone la conoscenza del *pin* di sblocco del dispositivo. Ciò, tuttavia, il più delle volte impone di ottenere la collaborazione dell'indagato (o di un terzo possessore del *device*), atteso che l'eventuale forzatura del dispositivo da parte delle forze dell'ordine – nel tentativo di indovinare la *password* – potrebbe cagionare la perdita definitiva di tutti i dati ivi contenuti[122]. Si pone, da questa prospettiva, il tema, più ampio, della rilevanza assunta dal diritto al silenzio e dal diritto contro l'autoincriminazione, a fronte di una richiesta di consegna della *password* da parte dell'autorità inquirente. A differenza della scelta compiuta in altri ordinamenti, tra cui proprio il Regno Unito, che si sono spinti così in là da concepire finanche degli obblighi penalmente sanzionati per coloro che non forniscano all'autorità informazioni utile a sbloccare il dispositivo[123], il Parlamento italiano si è finora del tutto disinteressato della questione, omettendo di fornire qualsivoglia indicazione, anche solo di matrice processuale, al riguardo[124]. Il che, peraltro, non stupisce data la criticabile inerzia che ancora oggi affligge il sistema processuale penale nostrano con riguardo alla più generale tematica del sequestro dei *device* digitali[125]; inerzia che, come è facile intuire, è foriera di significati-

[122] Si parla della c.d. funzionalità *wipe*. Nel caso di *Ledger*, per esempio, il sistema si resetta dopo tre tentativi falliti di inserimento del *pin*.

[123] Nella circolare *004/2024: Economic Crime and Corporate Transparency Act – cryptoasset confiscation order provisions*, 26 aprile 2024, attuativa della riforma del 2023, si precisa, infatti, che «appropriate officers have the power to require a person to provide information which is stored in electronic form», e che «if a person fails to comply with a requirement, then they may have committed an obstruction offence». Va, a ogni modo, precisato che, in virtù della nozione ampia del diritto al silenzio e di non collaborare sviluppata dalla Consulta (cfr., da ultimo, C. cost., 5 giugno 2023, n. 111), nel nostro ordinamento disposizioni di questo tenore si esporrebbero a inevitabili censure di legittimità costituzionale, per violazione del diritto del diritto di difesa.

[124] Cfr., sul punto, A. MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici… e non solo*, in *Proc. pen. giust.*, 2021, p. 729 ss.

[125] Si veda, al riguardo, il recente d.d.l. S 19 luglio 2023, n. 806 recante «Modifiche al codice di procedura penale in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali», volto a introdurre nel codice di rito un nuovo art. 254-*ter*. Cfr., al riguardo, il contributo di E. LORENZETTO in questo volume.

vi problemi applicativi nel contesto in esame proprio per l'importanza che gli applicativi informatici rivestono nel settore *de quo*.

Un'ulteriore tematica sulla quale occorre interrogarsi riguarda la possibilità di impiegare il captatore informatico quale mezzo di ricerca della prova occulto, al fine apprendere il *pin* di un dispositivo contenente la chiave privata di accesso al *wallet*, o finanche indirettamente quest'ultima. Mediante l'impiego della funzionalità c.d. *keylogger*, il *malware* – controllato in remoto dalle forze dell'ordine – consente, invero, teoricamente di acquisire in tempo reale tutto ciò che viene digitato sulla tastiera di un *device*[126] e, dunque pure una *password*. Tuttavia, come noto, il legislatore italiano ha disciplinato l'utilizzo della *trojan horse* solamente come peculiare modalità di intercettazione[127]. Non è stato regolamentato, invece, un impiego diverso, come il caso della modalità *online surveillance*, *online search* o, per l'appunto, della *keylogger function*. A fronte di ciò, occorre chiedersi se il semplice gesto di digitare una parola sul proprio *smartphone* o *computer* integri un vero e proprio comportamento comunicativo. In caso di risposta positiva, si potrebbe sostenere che il *pin* del dispositivo o finanche la chiave privata di un *wallet* ben potrebbero essere oggetto di intercettazione mediante *trojan* ai sensi dell'art. 266-*bis* c.p.p. Diversamente, l'utilizzo del *virus*, provocando un'ingerenza nel domicilio informatico tutelato all'art. 14 Cost.[128], dovrebbe ritenersi precluso, in base al principio per cui nel corso delle indagini penali tutto ciò che non è espressamente consentito

[126] Cfr. M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, Napoli, 2019, p. 200 ss.; W. NOCERINO, *Il captatore informatico nelle indagini interne e transfrontaliere*, Milano, 2021, p. 182.

[127] Si vedano, in proposito, M. MIRAGLIA, *Il "*Trojan *(non) di Stato": una disciplina da completare*, in *Processo penale e giustizia*, 2023, p. 1227 ss. e W. NOCERINO, *Il captatore informatico*, cit., p. 141 ss., a cui si rinvia anche per i cospicui riferimenti dottrinali e giurisprudenziali citati.

[128] Sull'esigenza di estendere la copertura dell'art. 14 Cost. anche al "domicilio informatico", v., da ultimo, le condivisibili considerazioni di M. MIRAGLIA, *Il "Trojan (non) di Stato"*, cit., p. 1227 ss.

dalla legge deve ritenersi vietato, perlomeno qualora il mezzo di ricerca della prova incida sui diritti fondamentali della persona[129].

Il tema è complesso, poiché la nozione di comunicazione, specialmente nell'era digitale, è assai controversa. Al riguardo, la giurisprudenza di legittimità, pur non avendo ancora assunto una posizione esplicita su questo specifico profilo, sembra offrire argomentazioni a favore della prima prospettazione or ora richiamata. In una recente pronuncia, infatti, la Corte di cassazione ha affermato che il comportamento consistente nella redazione di un *file Excel* sul proprio *computer*, «pur non costituendo una "comunicazione" in senso stretto, costituisce certamente, invece, un comportamento c.d. comunicativo, del quale è ammessa la captazione [mediante *trojan*]»[130]. La conclusione è stata giustificata in ragione del fatto che la semplice composizione di una parola sulla tastiera di un *electronic device* dovrebbe qualificarsi come un flusso unidirezionale di dati che transitano all'interno di un unico dispositivo. In altre parole, i giudici di legittimità sembrano identificare una condotta comunicativa nel "dialogo" che verrebbe a instaurarsi tra l'utente (*rectius*, la testiera del *computer*) e il sistema informatico centralizzato (il *software*). Volendo seguire questa interpretazione – con riguardo alla quale, però, la dottrina ha giustamente manifestato numerose perplessità[131] –, dovrebbe ritenersi ammissibile l'apprensione attraverso l'impiego del *malware* della chiave di accesso digitata sulla tastiera del *device* in uso al titolare del *wallet*.

Ma non è tutto. Ulteriori problemi si manifestano pure quando l'autorità inquirente sia riuscita a ottenere la chiave privata. L'indagato – o un suo complice – potrebbe aver copiato e archiviato (in formato digitale o cartaceo) la *password*, ovvero comunque averne la disponibilità da

[129] In questi termini, v. O. MAZZA, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Diritto penale contemporaneo - Rivista trimestrale*, 2013, 3, p. 4 ss.

[130] Cfr. Cass. pen, sez. I, sent. 1º febbraio 2021, n. 3591, in *OneLegale*.

[131] Si vedano, al riguardo, le osservazioni critiche mosse da L. ALGERI, *Lo* screenshot *eseguito (senza garanzie?) dal* Trojan *di Stato*, in *Giur. it.*, 2022, p. 2780 ss.; A. MALACARNE, *Il* trojan horse *"a cavallo" tra perquisizione e intercettazione: il problema del c.d.* screenshot *di file multimediali*, in *Diritto di internet*, 2022, p. 592 ss.; A. PROCACCINO, *Piccoli equivoci senza importanza: tra intercettazioni di flussi informatici, perquisizioni e prove atipiche*, in *Cass. pen.*, 2022, p. 3112 ss.

remoto, potendo così accedere al *wallet* e trasferire il "denaro" ivi presente altrove[132]. Inoltre, l'utilizzo del c.d. *backup recovery seed*[133], consentendo di recuperare in ogni momento il controllo delle somme legate a un *wallet*, a sua volta potrebbe permettere di eludere il vincolo reale imposto sul bene[134]. Quel che si vuole dire, è, in altre parole, che neppure l'ottenimento da parte degli investigatori della chiave di accesso garantisce l'ablazione definitiva della *res* e, dunque, non è sufficiente per eseguire un sequestro "a regola d'arte"[135].

La migliore soluzione a questo problema è quella di trasferire i fondi su un altro *wallet*, controllato direttamente dallo Stato. Si tratta, in effetti, della procedura prospettata nelle principali linee guida adottate in numerosi ordinamenti e dai più autorevoli organismi a livello internazionale[136], nonché, come si è accennato in precedenza, adottata dal legislatore britannico nell'*Economic Crime and Corporate Transparency Act 2023*. Epperò, anche in questo caso nel nostro ordinamento non è rintracciabile alcuna fonte di rango primario (e neppure secondario) che disciplini in maniera dettagliata l'*iter* procedimentale da seguire in dette circostanze. Di conseguenza, la scelta circa le modalità operative del sequestro è rimessa alla prassi, che si sta effettivamente sviluppando in modi affatto uniformi a seconda della singola autorità di contrasto chiamata a operare, con buona pace del principio di legalità processuale (art. 111, comma 1, Cost.)[137].

---

[132] Cfr. F. CAJANI, *Sequestri di* files *e* bitcoin, cit., p. 742, nt. 45; G. COSTABILE, *Le indagini digitali*, cit., p. 127.

[133] Si tratta di una sequenza di parole di *backup*, che serve all'utente per ripristinare l'accesso a un portafoglio.

[134] Cfr. D. KING, P. WARRACK, *Real considerations for law enforcement in seizing virtual currency*, 26 giugno 2016, all'indirizzo *https://www.acamstoday.org/real-considerations-for-law-enforcement-in-seizing-virtual-currency/*.

[135] V., al riguardo, P. DAL CHECCO, *Sequestro e confisca*, cit., p. 329.

[136] V. *supra*, nt. 106.

[137] Un problema delicato è, per esempio, come garantire la sicurezza delle cripto-attività apprese anche da eventuali attacchi di agenti infedeli (problema che si è posto negli USA già nel caso *Silk Road*). Onde risolvere tale questione, alcune forze di polizia hanno sviluppato la buona prassi non solo di videoregistrare le operazioni, ma anche di utilizzare *wallet* a firma multipla per poter spostare le cripto-attività, così da richiedere l'intervento di più soggetti contemporaneamente.

Ma anche laddove l'autorità inquirente riuscisse a eseguire lo spossessamento della *res*, l'estrema fluttuazione del valore delle criptomonete rende elevato il rischio di un loro improvviso deprezzamento. Il che risulta un problema di non poco conto, laddove vada eseguito un sequestro di tipo preventivo e conservativo[138]. Senza contare che si potrebbero porre spinose questioni in proposito in tutti i casi in cui la legge impone la restituzione del bene oggetto di sequestro[139].

Per far fronte alla volatilità delle criptomonete, le buone prassi di molti Stati europei consigliano, dopo aver trasferito, come detto, le monete virtuali in un *wallet* intestato alla procura o al tribunale, di convertirle in moneta FIAT, attraverso la vendita delle stesse nel mercato delle criptomonete[140]. Questa procedura presenta un triplice vantaggio: *i*) risolve alla radice il problema di un deprezzamento del suo valore nel caso in cui debba poi essere restituita; *ii*) evita il rischio che i *wallet* impiegati per custodire le criptomonete nel corso del procedimento siano oggetto di attacchi *cyber*, con conseguente perdita del denaro virtuale[141]; *iii*) consente, una volta operata la conversione, di intestare la moneta FIAT al Fondo Unico Giustizia[142].

Epperò, in assenza di una normativa *ad hoc*, è necessario chiedersi, *de iure condendo*, quale procedura debba essere seguita per la vendita e la conversione delle criptomonete.

---

[138] …atteso che, in detti casi, ciò che interessa è il "valore" equivalente del bene (*rectius*, la moneta virtuale) oggetto di apprensione. Nell'ipotesi del sequestro *ex* artt. 253 ss. c.p.p., invece, non sembrano profilarsi problemi di sorta, fino all'eventuale fase della confisca, atteso che tale mezzo di ricerca della prova è finalizzato a vincolare non il "valore" della cosa, ma la cosa in sé: cfr. R. LUPO, *Quale sequestro per le criptovalute?*, cit., p. 52.

[139] Al riguardo, infatti, occorre stabilire, per esempio, quale sia il valore oggetto di restituzione, ossia quello originario ovvero quello corrente, nonché individuare il soggetto chiamato eventualmente a rispondere per il deprezzamento subito dal bene.

[140] P. DAL CHECCO, *Sequestro e confisca*, cit., p. 344; F. CAJANI, *Sequestri di* files *e* bitcoin, cit., p. 743.

[141] Cfr. E. VALENTE, M. TORRE, *La regolamentazione delle "criptovalute": condotte illecite e strategie di contrasto*, in *Rivista di diritto privato*, 2019, p. 571; G. COSTABILE, *Le indagini digitali*, cit., p. 128.

[142] Si tratta di un profilo operativo di importanza chiave, dal momento che, a oggi, le cripto-attività non possono, in quanto tali, essere intestate al FUG.

Duplici sono, allo stato dell'arte, le opzioni astrattamente percorribili.

Si potrebbe, per un verso, ritenere applicabile l'art. 104-*bis* disp. att. c.p.p., il quale, come noto, stabilisce che nel caso in cui il sequestro preventivo[143] o la confisca abbiano a oggetto «beni», esclusi da quelli destinati a confluire nel Fondo Unico Giustizia, di cui è necessario assicurare l'amministrazione, l'autorità giudiziaria debba nominare un custode giudiziario o un amministratore giudiziario a cui affidare il compito della conversione, specie in caso di repentine fluttuazioni del mercato. Muovendosi in queste coordinate, sarebbe possibile ipotizzare di affidare a un terzo il potere di convertire, su richiesta, la moneta virtuale in valuta avente corso legale, nel caso in cui venisse ravvisato il pericolo di un imminente e brusco deprezzamento del bene.

Un'altra soluzione prospettabile è quella di applicare, in via analogica, la regolamentazione prevista all'art. 260, comma 3, c.p.p. relativa ai beni deperibili[144]. La disposizione prevede che, qualora le cose oggetto di sequestro[145] possano alterarsi – cioè, siano soggette a modificazione sostanziale o strutturale –, l'autorità giudiziaria debba disporne l'alienazione o la distruzione[146]. A tal proposito, non v'è dubbio che le criptoattività, pur non rappresentando, secondo alcuni, delle vere e proprie monete[147], debbano essere classificate come "beni", potendo dunque

[143] La norma si riferisce esplicitamente solo al sequestro preventivo, ma è pacifico che il suo raggio di applicazione possa estendersi anche al sequestro probatorio: in questi termini, v. pure F. CAJANI, *Sequestri di* files *e* bitcoin, cit., p. 743, nt. 50.

[144] Cfr. R. LUPO, *Quale sequestro per le criptovalute?*, cit., p. 53.

[145] Benché la disposizione richiami solamente il sequestro probatorio, la giurisprudenza ne ha esteso l'ambito di operatività pure al sequestro preventivo: Cass. pen., sez. III, 12 settembre 2018, n. 53341, in *OneLegale*.

[146] Al riguardo, la Cassazione ha stabilito che «la decisione dell'autorità giudiziaria di distruggere la cosa non ha natura di accertamento tecnico non ripetibile, suscettibile di applicazione delle modalità previste dall'art. 360». Si tratterebbe – secondo questa impostazione – di «un "semplice adempimento esecutivo", da realizzare senza particolari formalità. Ne discende, pertanto, che l'omissione dell'avviso al difensore non è in alcun modo sanzionabile, posto che l'art. 83 disp. att. lo prevede soltanto con riferimento ai prelievi di campioni»: Cass. pen., sez. III, 19 novembre 2019, n. 2202, in *OneLegale*.

[147] V., al riguardo, P. CARRIÈRE, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche di "strumenti finanziari", "valori mobiliari" e "prodotti finanziari";*

essere ricomprese nella sfera applicativa della disposizione. Così come non sembra potersi discutere la loro natura altamente volatile. Per di più, giova osservare come la giurisprudenza di legittimità abbia affermato che il concetto di deterioramento cui si riferisce la disposizione debba essere interpretato in senso ampio ed estensivo, potendo ricomprendere sia il caso di un deterioramento fisico del bene, sia un deprezzamento[148].

Entrambe le esegesi qui proposte, tuttavia, rappresentano una soluzione di compromesso, lasciando aperti diverse questioni di ordine pratico[149].

A fronte di un fenomeno così dirompente, le vigenti disposizioni codicistiche, quali quelle in tema di sequestro, si rivelano, in definitiva, inadeguate, richiedendo plurimi adattamenti su profili di rilievo cruciale. Il che, peraltro, non può stupire dal momento che esse sono state concepite per un contesto del tutto diverso rispetto all'ambiente iper-dinamico, nel quale vengono oggigiorno scambiati gli *asset* virtuali.

7. Conclusioni

A fronte di quanto osservato nel corso del presente lavoro, un dato è emerso con chiarezza: il tema del rapporto tra criminalità, giustizia penale e criptovalute deve necessariamente rappresentare una tematica prioritaria per il legislatore italiano. Ci troviamo, infatti, al cospetto di tecnologie che sono quotidianamente sfruttate dalle organizzazioni criminali per i loro traffici, causando problemi finanche di sicurezza nazionale.

Sul versante processual-penalistico, si è cercato di mettere in luce come le indagini che vedono coinvolte cripto-attività assumano spesso una natura molto articolata. Non solo esse hanno perlopiù matrice tran-

tra tradizione e innovazione, in *Riv. di diritto bancario*, 2019, p. 117 ss.; M. SEMERARO, *Moneta legale, moneta virtuale e rilevanza dei conflitti*, *ivi*, 2019, p. 237 ss.

[148] Cass. pen., sez. II, sent. 9 dicembre 2016, n. 1916, in *OneLegale*.

[149] La legge, per esempio, non individua il momento in cui andrebbe operata la conversione, né a quali *exchanges* dovrebbe rivolgersi l'autorità giudiziaria, né, ancora, quali e quante commissioni andrebbero pagate.

sazionale, ma richiedono pure l'impiego incrociato di plurimi strumenti di investigazione, tradizionali e di matrice altamente tecnologica. Con ciò si vuole dire che, per contrastare in modo efficace tutte le forme di criminalità che sfruttano il potenziale della *blockchain*, è indispensabile avere a disposizione un ecosistema normativo capace di affrontare le grandi sfide poste dalla criminalità contemporanea. Esso deve, infatti, permettere alle autorità di *law enforcement* di seguire in tempo reale e in tutto il globo i flussi di denaro criptati e, se del caso, di sequestrarli, in brevissimo tempo.

Sennonché, va preso atto che il nostro codice di procedura penale non risulta – a oggi – assolutamente all'altezza di questo presupposto di fondo. Da un lato, gli strumenti di indagine più tradizionali (quali, *in primis*, il sequestro probatorio) si rivelano inadeguati, non essendo calibrati sulla nuova realtà virtuale nella quale operano i "criminali 2.0". Dall'altro, il nostro codice, nonostante le critiche costantemente sollevate dalla dottrina[150], continua a non regolare affatto numerosi mezzi investigativi di stampo tecnologico (basti pensare, oltre ai già menzionati *software* di *blockchain forensic*, all'OSINT e al sequestro di *device*, al pedinamento GPS[151] e alle videoriprese investigative), con tutto ciò che ne consegue in termini di perdita di efficacia del sistema repressivo, così come di problemi di tutela dei diritti fondamentali. Al riguardo, i modelli cui ispirarsi – si pensi, per esempio, alla grande riforma compiuta in Spagna nel 2015[152] o, con specifico riguardo alle "*crypto-*

[150] In generale, sulla necessità di un intervento legislativo volto a regolamentare queste nuove strumentazioni investigative, v., pur con differenti prospettive di riforma, M. GIALUZ, *Premessa*, in ID.(a cura di), *Le nuove intercettazioni. Legge 28 febbraio 2020 n. 7*, in *Diritto di internet*, 2020, Supplemento al n. 3, p. 7; S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015, p. 789 ss.; F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Milano, 2020; e, volendo, J. DELLA TORRE, A. MALACARNE, *L'utilizzo dei* file di log *per scopi di contrasto alla criminalità: nodi problematici e possibili soluzioni*, in *archiviopenale.it* (rivista web), 22 dicembre 2023 (ultimo accesso il 28 febbraio 2025).

[151] Cfr. il contributo di S. SIGNORATO in questo volume.

[152] Il sistema processuale spagnolo è senz'altro all'avanguardia sul versante della regolamentazione dei moderni strumenti intrusivi impiegati nella fase delle indagini

indagini", al sistema recentemente implementato nel Regno Unito – sono ormai numerosi. Ciò che occorre, allora, è solo la buona volontà di seguirli.

Tuttavia, dobbiamo essere consapevoli del fatto che pure una riforma normativa sul fronte interno non potrebbe, di per sé, bastare.

Ulteriori sono i versanti sui quali è necessario intervenire.

Per un verso, è indispensabile sviluppare in questo settore un articolato piano di formazione continua e omogenea delle varie forze dell'ordine, così come della magistratura (e dell'avvocatura)[153]. E ciò dal momento che, come si è avuto modo di dimostrare, le indagini in esame richiedono una notevole dose di specializzazione da parte di tutti gli attori coinvolti e, in particolare, di coloro che sono chiamati a intervenire nelle prime battute dell'indagine.

A livello di autorità di *law enforcement*, un valido modello da seguire è, per esempio, quello sperimentato negli ultimi anni dall'Arma dei Carabinieri. A partire dal 2021, tale forza dell'ordine ha, infatti, per un verso, formato gruppi di agenti e ufficiali di polizia giudiziaria, dislocati nelle diverse parti del territorio nazionale, e, per un altro, creato una sezione specializzata nel settore, con sede a Roma, chiamata a occuparsi solo di queste fattispecie di reato, risolvendo i casi più complessi[154].

---

preliminari. Il riferimento corre alla *Ley Oganica* 5 ottobre 2015, n. 13, con la quale il legislatore ha modificato la *Ley de Enjuiciamiento Criminal* con il dichiarato obiettivo di disciplinare «las medidas de investigación tecnológica» e, contestualmente, rafforzare «las garantías procesales» dei soggetti coinvolti nell'accertamento. Per una panoramica sui contenuti della legge, v. F. BUENO DE MATA, *Las digilencia de investigacion penal en la cuarta revolucion industrial. Principios teoricos y problemas practicos*, Cizur Menor, 2019.

[153] Insistono giustamente sul punto, sin dall'inizio del loro *report*, N. TAMBÉ, A. OWEN, M. NIZZERO, *Crypto-Asset Recovery Challenges, Observed Practices and Strategies*, Londra, 2024, p. 1. V. anche le articolate raccomandazioni di EUROPOL e del BASEL INSTITUTE ON GOVERNANCE, *A race against time: Europol – Basel Institute on Governance recommendations on preventing and combating the criminal use of cryptocurrencies*, reperibili in *https://baselgovernance.org/publications/race-against-time-europol-basel-institute-governance-recommendations-preventing-and*.

[154] Trattasi della "Sezione Criptovalute del Comando Carabinieri Antifalsificazione Monetaria" che, come è dato leggere nel sito dell'Arma, è stata istituita il 4 ottobre 2021 «con il compito di contrastare le emergenti dinamiche criminali legate all'utilizzo illecito delle criptovalute e l'uso di piattaforme informatiche illegali per la vendita di

Questo modello "binario" pare vincente, perché capace di coniugare la diffusione di una conoscenza minima delle problematiche del settore agli operatori dislocati a livello locale, con la creazione di un corpo d'*élite*, in grado di fornire risposte proporzionate rispetto alle singole minacce in gioco.

Per altro verso, è essenziale potenziare anche i meccanismi di cooperazione internazionale[155]. L'esperienza maturata sul campo, infatti, insegna che le attività di contrasto rivelatesi maggiormente efficaci sono state quelle caratterizzate dall'operare congiunto di numerose forze appartenenti a diversi Stati membri[156].

Al riguardo, un *focus* specifico dovrebbe essere dedicato agli attuali sistemi di scambio informativo di polizia a livello europeo (quali, per esempio, SIRENE – *Supplementary Information Request at the National Entries*)[157], i quali dovrebbero essere aggiornati in modo tale da consentire un'interazione più celere ed efficace nell'ambito delle operazioni investigative digitali comuni.

Inoltre, è auspicabile, da un lato, incrementare gli sforzi per lo sviluppo di *software* di *blockchain analysis* "europei", creati *by design* in modo conforme all'*acquis* dell'Unione in materia di *privacy*, *data pro-*

valuta e altri prodotti contraffatti di specifica competenza del Comando» (*https://www.carabinieri.it/chi-siamo/oggi/organizzazione/mobile-e-speciale/comando-carabinieri-antifalsificazione-monetaria#:~:text=Il%204%20ottobre%202021%20%C3%A8,di%20valuta%20ed%20altri%20prodotti*).

[155] È questo, del resto, l'auspicio manifestato dagli stessi appartenenti alle forze dell'ordine che quotidianamente sono impegnati nell'attività di contrasto a questo tipo di criminalità: v. V. GIORDANO, *L'attività della Guardia di Finanza nell'ambito del sistema antiriciclaggio e il contrasto all'utilizzo dei* cryptoassets *per finalità illecite*, in *Rivista della Guardia di Finanza*, 2022, p. 512.

[156] Si veda, per esempio, l'operazione realizza da EUROPOL, in collaborazione con l'*European Financial and Economic Crime Centre* (EFECC), che ha portato al sequestro e alla confisca di ingenti somme in criptovalute di provenienza illecita (*https://www.europol.europa.eu/media-press/newsroom/news/europol-holds-largest-ever-operation-to-increase-seizures-of-criminal-assets-worldwide*).

[157] Ciascun Paese che utilizza il Sistema di Informazione Schengen-SIS ha istituito un ufficio SIRENE nazionale, operativo 24 ore al giorno, 7 giorni alla settimana, responsabile dello scambio di informazioni e del coordinamento delle attività connesse alle segnalazioni SIS.

tection e di intelligenza artificiale[158], nonché, dall'altro lato, dettare regole sovranazionali più avanzate in tema di sequestro e confische di *cripto-asset*, che coprano sia i profili procedurali dell'ablazione di tali beni, sia quelli di gestione e di vendita dei medesimi[159].

Fenomeni come quello della criminalità sulla *blockchain* dimostrano, insomma, come sia indispensabile aprire al più presto[160] un ambizioso cantiere di riforma, sia a livello italiano, sia europeo, dedicato al rapporto tra giustizia penale e tecnologie criptate. Solo così si potrà sperare di stare al passo delle organizzazioni criminali, evitando che continui a concretizzarsi quanto preconizzato, sul finire del secolo scorso, dai più cupi manifesti *Cypherpunk*, ovverosia che uno spettro continui a infestare «the modern world, the specter of crypto anarchy»[161].

[158] Da questa prospettiva, sicuramente un primo passo è costituito dalla recente pubblicazione della *call* HORIZON-CL3-2024-FCT-01-08, *Tracing of cryptocurrencies transactions related to criminal purposes*, la quale si propone di finanziare lo sviluppo di *software* di tracciamento delle cripto-attività specifici per le esigenze dell'Unione europea.

[159] Da questa prospettiva, sarebbe auspicabile creare una rete europea di agenzie statali, dotate di una serie di compiti in tema di gestione e di vendita di cripto-attività, in modo tale da ridurre i rischi (finanche di fallimento) degli operatori privati coinvolti in tali attività e di limitare gli esborsi economici (dovuti, per esempio, alle commissioni da pagare ai *provider*).

[160] Non a caso EUROPOL e il BASEL INSTITUTE ON GOVERNANCE nel titolo delle loro menzionate raccomandazioni (v. nt. 153) hanno fatto riferimento a una vera e propria "lotta contro il tempo".

[161] *The Crypto Anarchist Manifesto*, cit.

BACKDOOR NEI SISTEMI CRITTOGRAFICI TRA ESIGENZE DI SICUREZZA E DIRITTI UMANI

Antonino Alì

SOMMARIO: *1. Introduzione. 2. L'uso delle* backdoor *nella crittografia. 3. La Corte europea dei diritti dell'uomo e la crittografia. 4. Il caso* Telegram*: Podchasov contro la Russia. 5. Obblighi degli organizzatori di comunicazioni via Internet (ICO) e requisiti di decodifica per i servizi online nella Federazione Russa. 6. Le Nazioni Unite e l'Unione europea e l'importanza della crittografia. 7. Misure di conservazione dei dati e obbligo di fornire chiavi di decrittazione. 8. Un precedente rilevante sulla crittografia e la* privacy *digitale. 9. Il* First Report on Encryption *dell'*EU Innovation Lab *del 2024.*

1. Introduzione

Le tecniche crittografiche trovano ampie applicazioni nella tutela dell'integrità, della riservatezza e dell'autenticità delle informazioni. La tecnologia *blockchain*, per esempio, impiega strumenti crittografici per garantire che i messaggi non vengano alterati durante la trasmissione. La firma digitale assicura l'autenticità e la provenienza di un documento, rendendo verificabile l'identità del mittente. I protocolli Https utilizzano la crittografia per proteggere la trasmissione di dati sensibili nei siti *web*, come le credenziali di accesso o le informazioni bancarie. Anche le carte bancarie integrano meccanismi crittografici per proteggere le transazioni elettroniche da frodi e intercettazioni.

La cifratura, pilastro della crittografia, trasforma i dati in una forma illeggibile, accessibile solo a chi possiede la chiave. In sua assenza, decifrare è estremamente complesso: la solidità del sistema dipende principalmente dalla lunghezza della chiave e dalla complessità dell'algoritmo impiegato. Alcune tecniche si fondano su operazioni matematiche avanzate, altre su chiavi più brevi; in generale, maggiore è la complessità strutturale e la lunghezza della chiave, più elevata sarà la protezione garantita.

La questione dell'indebolimento della crittografia è un classico dilemma sicurezza/libertà che si è acuito nell'era digitale[1]. Da un lato, gli apparati di sicurezza degli Stati[2] sostengono di aver bisogno di accedere alle comunicazioni criptate per contrastare le minacce alla sicurezza nazionale, combattere la criminalità organizzata e proteggere i minori dagli abusi *online*, come dimostra il recente caso *EncroChat*[3]. D'altro

[1] Si veda J.A. LEWIS, D.E. ZHENG, W.A. CARTER, *The Effect of Encryption on Lawful Access to Communications and Data. A report of the CSIS Technology Policy Program*, New York-London, febbraio 2017; gli autori analizzano l'impatto del crescente uso della crittografia sulla capacità delle forze dell'ordine di accedere legalmente alle comunicazioni e ai dati. EUROPOL-EUROJUST, Terza relazione della funzione di osservatorio sulla crittografia, 2021 in *https://www.europol.europa.eu/cms/sites/default/files/documents/3rd_report_of_the_observatory_function_on_encryption-web.pdf*. Su questi temi vedi lo studio di G. ZICCARDI, *Crittografia e diritto. Crittografia, utilizzo e disciplina giuridica documento informatico e firma digitale, segretezza delle informazioni e sorveglianza globale*, Torino, 2003.

[2] In particolare, gli apparati di *intelligence* statali, attraverso collaborazioni interne ed esterne allo Stato, investono in tecnologie avanzate (soprattutto in potenza di calcolo) e influenzano il mercato crittografico commerciale per mantenere controllo e accessibilità. Questa strategia si basa sia su relazioni commerciali e cooperazione internazionale, sia sullo sviluppo di competenze multidisciplinari (informatica, matematica, crittografia) per rimanere sempre un passo avanti rispetto alle moderne tecnologie crittografiche. Si veda il documento "NSA's SIGINT Strategy, 2012-2016" pubblicato dal New York Times il 23 novembre 2013 (*A Strategy for Surveillance Powers https://archive.nytimes.com/www.nytimes.com/interactive/2013/11/23/us/politics/23nsa-sigint-strategy-document.html*). La strategia contiene obiettivi che sottolineano l'interesse strategico della *National Security Agency* a contrastare le sfide della crittografia per le sue missioni di *signal intelligence*; cfr. D.P. FIDLER (a cura di), *The Snowden Reader*, Bloomington, 2015, 170; cfr. U.S. HOUSE OF REPRESENTATIVES, *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden*, 2016, in *https://www.congress.gov/114/crpt/hrpt891/CRPT-114hrpt891.pdf*.

[3] Il caso ha avuto un risvolto giudiziario davanti alla Corte di giustizia dell'Unione europea (grande sezione), sent. 30 aprile 2024, causa C-670/22, *M.N. (EncroChat)*, ECLI:EU:C:2024:372. La Corte affronta l'uso di comunicazioni criptate intercettate nelle indagini penali transfrontaliere all'interno dell'Unione europea. Sebbene non tratti direttamente la questione delle *backdoor*, il caso evidenzia le sfide persistenti che le forze dell'ordine affrontano nell'intercettare e accedere alle comunicazioni crittografate utilizzate da potenziali criminali, come nel caso di servizi come *EncroChat*. La sentenza esamina la legalità dell'ottenimento e dell'utilizzo di dati provenienti da comunicazioni criptate, cercando di bilanciare i diritti alla privacy con le esigenze delle indagini pe-

canto, gli esperti di sicurezza informatica, i sostenitori dei diritti digitali e gran parte dell'industria tecnologica avvertono che compromettere l'integrità dei sistemi di crittografia comporterebbe rischi ben maggiori per la sicurezza collettiva e individuale[4]. Il problema è connaturato alla funzione primaria di una crittografia robusta: se implementata in modo efficace, impedisce l'accesso non autorizzato alle comunicazioni, senza distinguere tra malintenzionati e autorità governative[5].

2. L'uso delle backdoor *nella crittografia*

A prima vista, l'idea di consentire alle autorità di accedere ai dati crittografati aggirando la crittografia stessa può sembrare ragionevole.

---

nali nel contesto dell'Unione europea. Il caso ha avuto anche un risvolto davanti alla Corte eur. dir. uomo. Due cittadini britannici detenuti nel Regno Unito (ricorsi n. 44715/20 e 47930/21) hanno contestato il prelievo a distanza, da parte delle autorità francesi, dei dati di tutti i telefoni connessi alla rete *EncroChat* e il conseguente trasferimento di tali informazioni alle autorità del Regno Unito. I ricorrenti hanno messo in dubbio la qualità delle norme francesi che consentono il prelievo remoto dei dati e la necessità di tale misura. La Corte di Strasburgo (Corte eur. dir. uomo, sez. V, dec. 24 settembre 2024, *A.L. ed E.J. c. Francia*) ha dichiarato i ricorsi inammissibili perché i ricorrenti non avevano esaurito i rimedi interni in Francia. In particolare, ha rilevato che i dati *EncroChat*, già in possesso delle autorità francesi nell'ambito di un procedimento penale a Lille, erano stati trasferiti al Regno Unito come prova, su richiesta della *Crown Prosecution Service*, tramite un Ordine europeo di indagine penale (EIO). I ricorrenti avrebbero potuto contestare il trasferimento e l'utilizzo di tali dati in Francia in base all'articolo 694-41 del codice di procedura penale francese, ma non lo hanno fatto né hanno fornito motivazioni particolari per giustificare tale omissione. Cfr. R. STOYKOVA, *Encrochat: The hacker with a warrant and fair trials?*, in *Forensic Science International: Digital Investigation*, 2023, 46, 301602, che sottolinea le sfide che le forze dell'ordine devono affrontare nell'era delle tecnologie di crittografia avanzate.

[4] Si veda H. ABELSON, R. ANDERSON, S.M. BELLOVIN, J. BENALOH, M. BLAZE, W. DIFFIE, J. GILMORE, M. GREEN, S. LANDAU, P.G. NEUMANN, R.L. RIVEST, J.I. SCHILLER, B. SCHNEIER, M. SPECTER, D.J. WEITZNER, *Keys Under Doormats: mandating insecurity by requiring government access to all data and communication*, 7 luglio 2015, p. 8, in *https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf?ref=hackernoon.com*.

[5] Si veda B. SCHNEIER, *The value of encryption*, in *Schneier on Security*, April 2016, *https://www.schneier.com/essays/archives/2016/04/the_value_of_encrypt.html*.

Tuttavia, a un'analisi più attenta, vi sono aspetti critici che meritano un'attenta considerazione, soprattutto se si considerano le potenziali implicazioni a lungo termine. Da un punto di vista tecnico, l'introduzione di vulnerabilità intenzionali nei sistemi crittografici è piena di rischi[6].

La crittografia forte si basa su algoritmi matematici di tale complessità da sfidare anche le abilità degli esperti, rendendo virtualmente impossibile decifrare un messaggio senza la chiave corretta. L'implemen-

[6] Il caso Crypto AG, rivelato nel 2020, mostra come le *backdoor hardware* possano essere utilizzate per lo spionaggio su larga scala. L'operazione Rubicon, condotta dalla CIA e dal BND, ha permesso di manipolare i dispositivi di crittografia venduti da Crypto AG a oltre 120 Paesi, consentendo alle agenzie di intelligence di decifrare le comunicazioni segrete di molti governi. V. PARLAMENTO DELLA CONFEDERAZIONE SVIZZERA, *Affaire Crypto AG, Rapport de la Délégation des Commissions de gestion des Chambres fédérales du 2 novembre 2020*, in *https://www.parlament.ch/centers/documents/fr/bericht-gpdel-2020-11-10-f.pdf*; si veda anche G. MILLER, *How the CIA used Crypto AG encryption devices to spy on countries for decades*, Washington Post, 11 febbraio 2020, *https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/*. Analogamente, nel 2006 è emerso il caso dell'algoritmo Dual_EC_DRBG, proposto dall'NSA per l'uso nel settore pubblico. Nel 2007, due ricercatori di Microsoft hanno scoperto che l'algoritmo poteva contenere una *backdoor*, permettendo potenzialmente a chi ne conosceva i dettagli di prevederne l'output e di compromettere la sicurezza delle comunicazioni criptate. Entrambi i casi evidenziano come le *backdoor*, sia *hardware* che *software*, possano essere sfruttate per attività di spionaggio su larga scala, sollevando serie preoccupazioni per la sicurezza e la *privacy* delle comunicazioni globali. C. COMELLA, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza* Safe Harbor *della Corte di giustizia dell'Unione Europea*, in G. RESTA, Z. ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai* "principi di safe harbour" *allo* "scudo privacy", Roma, 2016, pp. 49-71. Inoltre, il caso del chip Clipper negli Stati Uniti negli anni Novanta illustra bene il dibattito sulle "*backdoor* di Stato" nei sistemi di crittografia. Questo chip, sviluppato su richiesta delle autorità governative, conteneva l'algoritmo Skipjack che permetteva di accedere ai dati criptati in caso di necessità. Nonostante le misure di sicurezza previste, come un numero di serie unico e un'unità di accesso legale, il progetto ha suscitato forti critiche. Le principali preoccupazioni riguardavano le potenziali vulnerabilità introdotte dalle *backdoor*, la difficoltà di implementare tali sistemi in modo sicuro e le implicazioni per la *privacy* e la sovranità dei dati. Queste preoccupazioni, unite alla mancanza di accettazione da parte del settore, hanno portato all'abbandono del progetto. Il caso del chip Clipper mette in evidenza le sfide e i rischi associati all'introduzione di *backdoor* nei sistemi di sicurezza, anche quando richiesto dalle autorità governative.

tazione di *backdoor* sicure è un'operazione complicata, anche per i crittografi più brillanti: anche se ben progettate, le backdoor possono essere scoperte e sfruttate[7].

L'introduzione di *backdoor* nei sistemi crittografici, sebbene possa sembrare una soluzione pragmatica per facilitare l'accesso delle autorità competenti, comporta rischi significativi. Tali vulnerabilità possono compromettere l'integrità dei sistemi, esponendo milioni di utenti a potenziali minacce e minando la fiducia nella sicurezza delle comunicazioni digitali, fondamentali per settori come il commercio elettronico e i servizi finanziari[8]. La semplice ipotesi dell'esistenza di *backdoor* può generare sospetti e timori tra gli utenti. Inoltre, categorie particolarmente vulnerabili, come giornalisti e attivisti, dipendono da una crittografia robusta per operare in sicurezza; un suo indebolimento potrebbe esporli a gravi pericoli. Pertanto, l'implementazione di *backdoor* richiede un'attenta valutazione dei rischi e dei benefici, considerando le implicazioni sulla sicurezza complessiva dei sistemi e sulla fiducia degli utenti.

3. La Corte europea dei diritti dell'uomo e la crittografia

La progressiva normalizzazione della sorveglianza elettronica[9] e le relative contromisure rappresentano un fenomeno centrale nell'era digi-

[7] Si veda B.J. NIXON, *The Case for Mandatory Encryption Backdoor Legislation: Sabotaging the Right to Privacy or a Necessary Measure to Address the 'Going Dark' Problem?*, in *Complex*, 2021, che esamina le crescenti pressioni per introdurre una legislazione che imponga *backdoor* di crittografia per consentire alle forze dell'ordine di accedere ai dati crittografati.

[8] Si veda K.W. DAM, H.S. LIN (eds.), *Cryptography's Role in Securing the information society*, Committee to Study National Cryptography Policy, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academy Press, Washington, D.C., 1996, in *https://nap.nationalacademies.org/read/5131/chapter/1*.

[9] La "normalizzazione della sorveglianza" si riferisce al processo attraverso il quale le pratiche di sorveglianza su vasta scala vengono gradualmente accettate e integrate nei quadri giuridici e sociali. In questo contesto, la Corte di giustizia europea, attraverso una serie di sentenze, ha stabilito la legittimità della "raccolta massiva di dati" a determinate condizioni, con l'obiettivo di prevenire gli abusi di potere. La Corte ha stabilito

tale, segnato da un momento cruciale: le rivelazioni di Edward Snowden nel 2013, che hanno svelato l'estensione delle attività di spionaggio condotte soprattutto da intelligence statunitense e britannica[10].

L'adozione su larga scala della crittografia *end-to-end* (E2E) rappresenta una risposta alla massiccia raccolta di dati nel settore pubblico e in quello privato. La crittografia *end-to-end* è un sistema di cifratura delle comunicazioni in cui solo il mittente e il destinatario possono leggere il contenuto del messaggio. Il principio fondamentale è che i dati vengono cifrati sul dispositivo del mittente e decifrati solo sul dispositivo del destinatario, senza che nessun altro – nemmeno il fornitore del servizio (come *WhatsApp*, *Signal* o *iMessage*) – possa accedervi durante il transito.

Numerosi fornitori di messaggistica istantanea hanno adottato la crittografia *end-to-end* nei propri servizi di messaggistica e videocomunicazione, riconoscendone il valore centrale nella tutela della privacy degli utenti. Alcune di esse hanno implementato questa tecnologia per la totalità dei messaggi scambiati sulle loro piattaforme, rendendo inaccessibile il contenuto delle comunicazioni anche ai gestori del servizio.

---

requisiti specifici per la legalità di tali pratiche, tra cui: una base giuridica chiara e accessibile, la proporzionalità e la necessità della misura, una supervisione indipendente e garanzie procedurali per i diritti individuali. Queste sentenze hanno contribuito a creare un quadro giuridico che, pur riconoscendo la potenziale utilità della sorveglianza di massa per la sicurezza nazionale, cerca di trovare un equilibrio con la protezione dei diritti fondamentali dei cittadini. Cfr. Corte eur. dir. uomo, grande camera, sent. 25 maggio 2021, Big Brother Watch e altri c. Regno Unito; M. MILANOVICH, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa*, in *https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/*; E. WATT, *State sponsored cyber surveillance: the right to privacy of communications and international law*, Cheltenham, 2021.

[10] Per una panoramica sulle questioni relative alla crittografia e ai diritti umani, si veda W. SCHULZ, J. VAN HOBOKEN (eds.), *Human rights and Encryption*, UNESCO Internet Freedom Series, 2016; si veda anche S. MILLER, *Privacy, Encryption and Counter-Terrorism*, in A. HENSCHKE, A. REED, S. ROBBINS, S. MILLER (eds.), *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*, Cham, 2021, pp. 139-154 e nello stesso volume T. BOSSOMAIER, K. MACNISH, *An End to Encryption? Surveillance and Proportionality in the Crypto-Wars*, pp. 155-175.

Altre hanno invece potenziato la sicurezza dei servizi di posta elettronica, introducendo funzionalità avanzate volte ad accrescere la riservatezza dei messaggi.

Tali misure proteggono i contenuti, ma i metadati restano accessibili ai fornitori. La crescente attenzione verso forme avanzate di sicurezza digitale ha inevitabilmente generato tensioni con le autorità governative, in particolare nei sistemi democratici in cui coesistono esigenze di sicurezza nazionale e tutela dei diritti fondamentali. Negli Stati Uniti, per esempio, il *Federal Bureau of Investigat*ion ha più volte manifestato preoccupazioni in merito all'uso diffuso della crittografia forte, ritenendola un ostacolo concreto alle attività investigative[11].

Questa tensione ha alimentato un acceso dibattito sull'introduzione di *backdoor* nei sistemi crittografici, una proposta fortemente contestata sia dalle aziende tecnologiche che dagli attivisti per la tutela della privacy (le c.d. *Crypto wars*)[12].

[11] Il caso *Apple* legato alla strage di San Bernardino del 2016 ha evidenziato il complesso equilibrio tra sicurezza nazionale e *privacy* digitale. Quando l'FBI ha chiesto ad *Apple* di creare un *software* per sbloccare il telefono di uno degli attentatori, l'azienda si è opposta fermamente (si veda APPLE, Customer Letter del 16 febbraio 2016, all'indirizzo *https://www.apple.com/customer-letter/*). *Apple* ha sostenuto che non solo era tecnicamente impossibile aggirare la crittografia dei suoi dispositivi, ma che la creazione di una *backdoor* avrebbe compromesso la sicurezza di tutti i suoi prodotti. Questa posizione rifletteva la più ampia preoccupazione di *Apple* per la *privacy* dei suoi utenti. Anche se alla fine l'FBI è riuscita a sbloccare il telefono attraverso una terza parte, il caso ha riacceso il dibattito sull'accesso del governo alla crittografia forte. L'episodio ha evidenziato la continua tensione tra le esigenze investigative delle forze dell'ordine e la necessità di proteggere la *privacy* degli utenti di tecnologie criptate, sollevando questioni cruciali sul futuro della sicurezza digitale e dei diritti individuali nell'era tecnologica. Si veda M. SALA, *La crittografia al centro dello scontro tra Apple e Fbi*, in *Gnosis*, 2015, 2, pp. 139-143.

[12] Le *crypto wars* sono state una lunga serie di conflitti, iniziati negli anni Settanta, tra governi e difensori della *privacy* digitale riguardo all'uso della crittografia. Cfr. C. JARVIS, *Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption*, Boca Raton, 2020.

4. Il caso Telegram*: Podchasov contro la Russia*

Una sentenza della Corte eur. dir. uomo ha di recente sollevato questioni fondamentali sul delicato equilibrio tra sicurezza nazionale e diritti individuali alla *privacy* e alla libertà di espressione nell'era digitale[13]. *Telegram*, un'applicazione di messaggistica istantanea nota per la sua enfasi sulla *privacy* e sulla sicurezza attraverso la crittografia, si è trovata al centro di una controversia legale con il Servizio di sicurezza federale della Federazione russa (FSB). Il caso si colloca in un contesto normativo complesso, in cui la legislazione russa impone agli organizzatori di comunicazioni via Internet obblighi rigorosi di conservazione e accesso ai dati, inclusa la decifrabilità delle comunicazioni criptate su richiesta delle autorità.

La controversia è nata quando l'FSB ha chiesto a *Telegram* di fornire i dati necessari per decriptare le comunicazioni di alcuni utenti sospettati di essere coinvolti in attività terroristiche. La società ha rifiutato, sostenendo che la consegna delle chiavi crittografiche avrebbe compromesso la sicurezza e la *privacy* dell'intera piattaforma. In risposta al rifiuto di *Telegram*, le autorità russe hanno imposto multe e ordinato il blocco dell'applicazione sul territorio russo.

Anton Valeryevich Podchasov, utente della piattaforma *Telegram*, ha presentato ricorso contro la Federazione Russa alla Corte europea dei diritti dell'uomo il 18 giugno 2019, dopo aver esaurito i rimedi giurisdizionali interni. La vicenda si è svolta alcuni anni prima del ritiro della Russia dal Consiglio d'Europa e dalla Convenzione europea dei diritti dell'uomo. Podchasov, insieme ad altri trentaquattro ricorrenti, ha impugnato un ordine di divulgazione emanato dal Servizio di sicurezza federale (FSB), con cui si richiedeva a *Telegram* di fornire informazioni

[13] Corte eur. dir. uomo, sez. III, sent. 13 febbraio 2024, Podchasov c. Russia. Sul caso v. R. LAKRA, *Cracking the Code: How Podchasov v. Russia Upholds Encryption and Reshapes Surveillance*, in *EJIL: Talk*, 13 marzo 2024; A. STIANO, *Utilizzo della crittografia, backdoor e accesso alle comunicazioni digitali: brevi considerazioni a margine della sentenza Podchasov c. Russia*, in *SidiBlog*, 26 marzo 2024, *http://www.sidiblog.org/2024/03/26/utilizzo-della-crittografia-backdoor-e-accesso-alle-comunicazioni-digitali-brevi-considerazioni-a-margine-della-sentenza-podchasov-c-russia/*.

tecniche idonee a decriptare le comunicazioni di utenti sospettati di attività terroristiche.

Secondo i ricorrenti, la consegna delle chiavi di crittografia avrebbe consentito al FSB di accedere potenzialmente a tutte le comunicazioni veicolate attraverso la piattaforma, violando il diritto alla privacy e alla riservatezza delle comunicazioni garantito dall'articolo 8 della Convenzione.

Il 25 febbraio 2022, il Comitato dei Ministri del Consiglio d'Europa ha sospeso il diritto di rappresentanza della Federazione Russa all'interno dell'organizzazione, in risposta all'aggressione armata contro l'Ucraina, considerata una grave violazione degli obblighi derivanti dallo Statuto del Consiglio. Successivamente, il 15 marzo 2022, la Russia ha notificato formalmente al Segretario generale del Consiglio d'Europa il proprio recesso dall'organizzazione ai sensi dell'articolo 7 dello Statuto, esprimendo contestualmente l'intenzione di denunciare la Convenzione europea dei diritti dell'uomo. Il giorno seguente, il 16 marzo 2022, il Comitato dei Ministri ha deliberato l'espulsione immediata della Federazione Russa dal Consiglio d'Europa, ponendo fine a 26 anni di appartenenza all'organizzazione. La cessazione dell'appartenenza della Russia alla Convenzione europea dei diritti dell'uomo è divenuta effettiva il 16 settembre 2022, sei mesi dopo la notifica di recesso, conformemente all'articolo 58 della Convenzione. L'espulsione della Russia dal Consiglio d'Europa il 16 marzo 2022, a seguito dell'invasione dell'Ucraina, ha dato inizio al processo di cessazione dell'adesione della Russia alla Conv. eur. dir. uomo[14].

È stato, tuttavia, stabilito un periodo transitorio di sei mesi, dal 16 marzo al 16 settembre 2022, durante il quale la Corte di Strasburgo ha mantenuto la giurisdizione sui casi contro la Russia relativi a eventi verificatisi entro la fine di tale periodo[15]. Il 5 settembre 2022, la sessio-

[14] Cfr. la Risoluzione CM/Res(2022)2 sulla cessazione della qualità di membro della Federazione Russa al Consiglio d'Europa, adottata dal Comitato dei Ministri il 16 marzo 2022 (*https://search.coe.int/cm?i=0900001680a5da51*); e le osservazioni critiche di L. BORLINI, *L'espulsione della Federazione Russa dal Consiglio d'Europa e le conseguenze giuridiche della cessazione della qualità di membro*, in *RDI*, 2023, p. 37.

[15] Il 22 marzo 2022, la Corte plenaria ha adottato una risoluzione sulle conseguenze del ritiro della Russia dal Consiglio d'Europa. Questa risoluzione, basata sull'articolo

ne plenaria della Corte europea dei diritti dell'uomo ha formalizzato questo principio, affermando che essa avrebbe mantenuto la giurisdizione per esaminare le domande contro la Russia in relazione ad atti od omissioni avvenuti fino al 16 settembre 2022[16].

Gli eventi oggetto del caso Podchasov, compresa l'adozione della normativa contestata e le condotte delle autorità russe, si sono svolti prima del 16 settembre 2022, data entro cui la Corte europea dei diritti dell'uomo ha conservato la propria giurisdizione nei confronti della Federazione Russa. Inoltre, poiché entrambe le parti avevano già depositato le rispettive osservazioni prima del ritiro ufficiale della Russia dalla Convenzione, la Corte ha potuto proseguire l'esame del ricorso senza ostacoli procedurali.

5. Obblighi degli organizzatori di comunicazioni via Internet (ICO) e requisiti di decodifica per i servizi online nella Federazione Russa

Negli corso dell'ultimo decennio, la Russia ha introdotto modifiche sostanziali alla legislazione sull'informazione, con particolare attenzione alle comunicazioni *online*. Le leggi federali russe n. 374-FZ e 375-FZ del 6 luglio 2016, comunemente note come "pacchetto Yarovaya", si inseriscono in un più ampio processo di revisione normativa volto a rafforzare le misure antiterrorismo e la sicurezza pubblica, e sono strettamente connesse alla legge federale n. 149-FZ del 27 luglio 2006, che costituisce il quadro generale in materia di informazione, tecnologie dell'informazione e protezione dei dati.

---

58 della Convenzione europea dei diritti dell'uomo, stabiliva che lo *status* della Federazione russa come Alta Parte contraente della Convenzione sarebbe terminato il 16 settembre 2022. Secondo l'interpretazione prevalente dell'articolo 58 della Convenzione, la Conv. eur. dir. uomo ha continuato ad applicarsi alla Russia per un periodo di sei mesi dopo la cessazione dello *status* di membro del Consiglio d'Europa, quindi fino al 16 settembre 2022.

[16] Il 5 settembre 2022, la Corte plenaria ha ufficialmente riconosciuto che la posizione di giudice per la Federazione Russa sarebbe terminata a partire dal 16 settembre 2022. Di conseguenza, l'elenco dei giudici *ad hoc* idonei a giudicare le cause contro la Russia non è più valido.

Il pacchetto ha introdotto modifiche sostanziali alla 149-FZ, imponendo, in particolare con la legge 374-FZ, obblighi stringenti per i fornitori di servizi di telecomunicazione e per le piattaforme digitali, tra cui la conservazione obbligatoria, per sei mesi, dei contenuti delle comunicazioni elettroniche (inclusi messaggi vocali, testi, immagini e video) e, per un periodo fino a tre anni, dei relativi metadati. Tali dati devono essere archiviati all'interno del territorio della Federazione Russa e resi accessibili alle autorità competenti su richiesta. Le modifiche apportate alla 149-FZ hanno rafforzato il sistema normativo in materia di sicurezza informativa, intensificando gli obblighi di cooperazione con i servizi di sicurezza.

Le responsabilità imposte agli "organizzatori di comunicazioni via Internet" (ICO) dalla normativa russa sono particolarmente gravose e incidono in modo rilevante sulla *privacy online*. Il fulcro della disciplina normativa risiede negli obblighi di conservazione dei dati: gli ICO sono tenuti a conservare i metadati relativi alle comunicazioni degli utenti per dodici mesi. Questi metadati comprendono informazioni quali l'ora, la data e la durata delle comunicazioni, nonché le identità dei soggetti coinvolti. Agli ICO viene, inoltre, domandata la conservazione integrale del contenuto effettivo di tutte le comunicazioni per sei mesi. Questo obbligo si estende a testi, registrazioni vocali, immagini e qualsiasi altro tipo di contenuto scambiato dagli utenti, determinando una sorveglianza pervasiva e potenzialmente lesiva dei diritti fondamentali degli utenti.

Queste disposizioni sollevano importanti interrogativi sulla protezione della *privacy* e della libertà di comunicazione *online* in Russia. In effetti, la legge impone agli ICO di fornire alle autorità le informazioni necessarie per decifrare le comunicazioni criptate, obbligandole in sostanza a compromettere la sicurezza dei loro sistemi e a consegnare le chiavi di decifrazione su richiesta. Le implicazioni tecniche della normativa russa sono significative. Le ICO devono non solo garantire che le loro apparecchiature soddisfino i requisiti tecnici specifici stabiliti dal governo, ma anche a collaborare attivamente con le autorità, facilitandone l'accesso ai sistemi. In concreto, ciò potrebbe significare l'integrazione di tecnologie di sorveglianza direttamente nell'infrastruttura di comunicazione. Per i servizi di messaggistica istantanea, le restrizioni

sono ancora più stringenti: oltre a tutti gli altri requisiti, questi servizi devono identificare i loro utenti attraverso il loro numero di telefono cellulare, rendendo di fatto impraticabile l'utilizzo anonimo di tali piattaforme.

Un aspetto particolarmente controverso della normativa è l'obbligo imposto agli ICO di fornire alle autorità, su richiesta, le chiavi di decrittazione necessarie per accedere alle comunicazioni cifrate. In presenza di sistemi di crittografia *end-to-end*, ciò implica che le aziende devono predisporre i mezzi tecnici per rendere leggibili i contenuti protetti, con gravi implicazioni sia per la riservatezza delle comunicazioni degli utenti, sia per la sicurezza complessiva delle infrastrutture digitali.

La legge mira a rafforzare la sicurezza nazionale e a contrastare il terrorismo. L'obbligo di fornire le chiavi di decrittazione ha rappresentato, di fatto, una minaccia diretta alla crittografia *end-to-end*, compromettendo la riservatezza delle comunicazioni private e minando uno degli strumenti fondamentali per la tutela della sicurezza digitale e dei diritti fondamentali degli utenti. Per molti operatori del settore, adempiere a tale obbligo risultava tecnicamente complesso, se non impossibile, senza compromettere la sicurezza dell'intero sistema di comunicazione. Questa problematica ha messo in luce il conflitto tra le esigenze di sicurezza nazionale e la tutela della *privacy* digitale, evidenziando le difficoltà pratiche e normative nel bilanciare questi interessi contrapposti.

È in questo contesto complesso che si inserisce il caso *Podchasov c. Russia*, il quale ha spinto la Corte eur. dir. uomo a esaminare la compatibilità di tali misure con il diritto alla *privacy* sancito dall'articolo 8 Cedu. Questo caso assume un ruolo centrale nel dibattito sulla regolamentazione della crittografia e sulla tutela dei dati personali nell'era digitale, sollevando questioni fondamentali sull'equilibrio tra sicurezza nazionale e protezione delle libertà individuali.

6. Le Nazioni Unite e l'Unione europea e l'importanza della crittografia

Nel caso *Podchasov c. Russia*, la Corte europea richiama vari strumenti internazionali a sostegno della propria posizione in difesa della

crittografia quale elemento essenziale per la tutela della *privacy* e della libertà di espressione nell'era digitale[17].

Richiama in primo luogo il rapporto 2022 dell'Alto Commissario delle Nazioni Unite per i diritti umani che riconosce la crittografia non solo come uno strumento tecnico, ma come una garanzia essenziale dei diritti fondamentali. Il rapporto sottolinea il ruolo della crittografia nel proteggere la libertà di comunicazione e mette in guardia contro le restrizioni governative sulla crittografia, avvertendo che tali misure possono avere effetti negativi sproporzionati sull'intera popolazione[18].

---

[17] Cfr. OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS, *The right to privacy in the digital age*, Report of the Office of the United Nations High Commissioner for Human Rights, Human Rights Council, fifty-first session, 2022, in *https://docs.un.org/en/A/HRC/51/17*.

[18] Pur non menzionato esplicitamente nella sentenza, è rilevante richiamare quanto osservato nel 2018 dal relatore speciale ONU David Kaye nel "Rapporto di *follow-up* su crittografia e anonimato", in tema di libertà di espressione e protezione della *privacy*. Cfr. A/HRC/38/35/Add.5, in *https://digitallibrary.un.org/record/1638475/files/A_HRC_38_35_Add-5-EN.pdf*. Rapporto del Relatore speciale sulla promozione e la protezione del diritto alla libertà di opinione e di espressione come follow-up del rapporto 2015 sull'uso della crittografia e dell'anonimato per esercitare i diritti alla libertà di opinione e di espressione nell'era digitale (A/HRC/29/32) (A/HRC/29/32), in *https://digitallibrary.un.org/record/1638475/files/A_HRC_38_35_Add-5-EN.pdf*. Quest'ultimo rapporto si è concentrato sulle modalità di utilizzo degli strumenti di crittografia e anonimato per esercitare la libertà di opinione e di espressione nel regno digitale. Negli anni successivi al 2015, il panorama si è evoluto in modo significativo e sono emerse due tendenze contrastanti: un aumento delle restrizioni imposte dai governi alle tecnologie di crittografia e una crescente enfasi sulle misure di sicurezza digitale all'interno di settori chiave dell'industria delle tecnologie dell'informazione e della comunicazione (TIC). Vedi anche *UCI Law International Justice Clinic, "Selected references: unofficial companion to report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and the freedom of expression"*, in *https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/States/Selected_References_SR_Report.pdf*. Il relatore speciale David Kaye, nel rapporto del 2018, ha delineato un quadro allarmante sulle restrizioni governative alla crittografia, spesso adottate in violazione dei principi di necessità e proporzionalità previsti dal diritto internazionale dei diritti umani. Secondo il Relatore, tali misure – dal divieto totale all'indebolimento degli standard di sicurezza o all'imposizione di sistemi di deposito delle chiavi – compromettono gravemente la *privacy*, la libertà di espressione, il giusto processo e, in alcuni casi, la sicurezza fisica degli individui. Il rapporto denuncia anche la carenza di dibattito pubblico e di impegno da parte delle istituzioni internazionali, del settore privato e della società civile nella promozione della

La posizione favorevole alla crittografia è sostenuta da atti ufficiali del Consiglio d'Europa. La Raccomandazione del Comitato dei Ministri del 2012 incoraggia esplicitamente l'uso della crittografia *end-to-end* nei servizi di *social network*, riconoscendola come uno strumento essenziale per la protezione della *privacy online*. A questa si aggiunge la Risoluzione dell'Assemblea parlamentare del 2015, che esprime preoccupazione per le pratiche di taluni servizi di intelligence volte a indebolire i sistemi di sicurezza. La risoluzione sottolinea i rischi che derivano dall'indebolimento della crittografia, non solo per la riservatezza delle comunicazioni individuali, ma anche per la sicurezza collettiva di fronte a minacce come il terrorismo e la criminalità informatica[19].

La Corte richiama alcune decisioni della Corte di giustizia dell'Unione europea, le quali affermano che l'accesso indiscriminato ai contenuti delle comunicazioni elettroniche è incompatibile con i diritti fondamentali garantiti dalla Carta dell'Unione[20]. A queste si affianca la dichiarazione congiunta di *Europol* ed ENISA (*European Union Agency for Cybersecurity*) del 2016 offre una prospettiva pratica, riconoscendo la necessità di bilanciare le esigenze investigative con la protezione della *privacy*[21]. Questo documento sconsiglia l'introduzione di *backdoor* obbligatorie o di sistemi di deposito di chiavi, sottolineando come tali misure possano indebolire la sicurezza generale ed essere facilmente aggirate dai criminali. In linea con questa prospettiva, il parere congiunto dell'*European Data Protection Board* e dell'*European Data Protection Supervisor* (EDPB-EDPS)del 2022 ribadisce il ruolo cruciale della crit-

sicurezza digitale. Secondo Kaye, l'assenza di un approccio equilibrato rischia di dar luogo a un ecosistema digitale ostile alla libertà e ai diritti fondamentali.

[19] ASSEMBLEA PARLAMENTARE DEL CONSIGLIO D'EUROPA, Risoluzione 2045 (2015), in *https://pace.coe.int/files/21692/pdf*.

[20] CGUE, grande sezione, sent. 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd e a.* contro *Minister for Communications, Marine and Natural Resources e a.*, ECLI:EU:C:2014:238. CGUE, grande sezione, sent. 6 ottobre 2015, causa C-362/14, *Maximillian Schrems contro Data Protection Commissioner*, ECLI: EU:C:2015:650.

[21] Vedere *https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection* e *https://www.europol.europa.eu/cms/sites/default/files/documents/on_lawful_criminal_investigation_respecting_21st_century…%20%281%29.pdf*.

tografia, avvertendo che qualsiasi intervento normativo volto a indebolirla potrebbe compromettere non solo la *privacy*, ma anche la libertà di espressione e lo sviluppo dell'innovazione digitale in Europa.[22].

Nel complesso, le fonti citate confermano il consenso internazionale sul ruolo essenziale della crittografia per i diritti umani e i rischi legati al suo indebolimento, evidenziando come la Corte di Strasburgo abbia fondato la sua decisione su un ampio quadro normativo e istituzionale.

7. Misure di conservazione dei dati e obbligo di fornire chiavi di decrittazione

La Corte ha ritenuto che la normativa russa violasse l'art. 8 Cedu, che tutela il diritto alla *privacy* e alla corrispondenza, per tre motivi principali. In primo luogo, la Corte ha evidenziato che l'obbligo imposto ai fornitori di servizi di comunicazione di conservare indiscriminatamente i dati relativi a tutti gli utenti di Internet – a prescindere da qualsiasi sospetto o coinvolgimento in attività illecite – costituisce un'ingerenza eccezionalmente ampia e grave nel diritto alla *privacy*. Si tratta di una misura di sorveglianza preventiva e generalizzata che, proprio perché prescinde da qualsiasi criterio di selettività o proporzionalità. In secondo luogo, la Corte ha rilevato la mancanza di garanzie adeguate contro l'abuso nell'accesso ai dati da parte delle autorità pubbliche. In particolare, ha evidenziato l'assenza di un meccanismo di autorizzazione preventiva da parte di un organo indipendente, come un giudice o un'autorità amministrativa imparziale. Infine, la Corte ha ritenuto sproporzionato l'obbligo, previsto dalla normativa, di consentire alle autorità l'accesso alle comunicazioni cifrate *end-to-end* mediante la fornitura delle relative chiavi di decrittazione. Questa disposizione, ha osservato la Corte, compromette strutturalmente la sicurezza delle comunicazioni elettroniche, poiché l'indebolimento generalizzato della crittografia – anche con finalità investigative – espone tutti gli utenti, indistintamente, a potenziali rischi di intrusione, sorveglianza e abuso.

[22] *https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf*.

Questa sentenza rappresenta un progresso fondamentale nella tutela della privacy digitale, in quanto sancisce con chiarezza il principio secondo cui una crittografia solida e inviolabile è elemento imprescindibile per garantire la protezione dei diritti fondamentali nell'era digitale. La Corte ha sottolineato che esistono metodi alternativi di indagine meno invasivi rispetto all'imposizione di *backdoor* nei sistemi crittografici.

La crittografia *end-to-end* è costituisce oggi uno degli ultimi baluardi per la protezione della privacy e la sicurezza delle comunicazioni digitali. Obbligare i fornitori di servizi a indebolire questa protezione o a introdurre *backdoor* compromette la riservatezza delle comunicazioni, esponendo tutti gli utenti a potenziali rischi di sorveglianza di massa.

La Corte ha sottolineato l'estensione e la gravità dell'interferenza determinata dalla legislazione contestata (§ 70). La legislazione russa prevedeva la conservazione automatica e continua del contenuto (non dei soli metadati) di tutte le comunicazioni via Internet per sei mesi e dei relativi dati di traffico per un anno. Tale misura, ha rilevato la Corte, si applicava indiscriminatamente a tutti gli utenti delle comunicazioni online, indipendentemente da qualsiasi sospetto di attività criminale. Inoltre, la conservazione riguardava l'intero contenuto delle comunicazioni, senza alcuna limitazione in termini di ambito territoriale, durata o categorie di persone interessate.

La Corte eur. dir. uomo, nell'esaminare le conseguenze derivanti dalla compromissione dei sistemi crittografici, ha sottolineato che per decriptare le comunicazioni protette dalla crittografia *end-to-end*, come *Telegram*, non potrebbe essere limitata a singoli individui. I giudici di Strasburgo affermano che

> l'indebolimento della crittografia mediante la creazione di *backdoor* renderebbe apparentemente tecnicamente possibile la sorveglianza di routine, generale e indiscriminata delle comunicazioni elettroniche personali (§ 77).

Peraltro, l'introduzione di *backdoor* nei sistemi di comunicazione, potrebbe essere sfruttata anche da attori malevoli e rappresenterebbe un vulnus per la sicurezza delle comunicazioni elettroniche di tutti gli utenti.

8. Un precedente rilevante sulla crittografia e la privacy *digitale*

La sentenza fin qui analizzata rappresenta un precedente rilevante nel dibattito europeo in materia di tutela della *privacy* digitale e protezione della sicurezza nazionale. La Corte ha sottolineato il ruolo fondamentale della crittografia robusta nella salvaguardia della vita privata e dell'integrità dei sistemi informatici, opponendosi a orientamenti normativi volti a indebolire tali meccanismi di protezione.

Pur riconoscendo che la crittografia possa costituire un ostacolo per le attività investigative, la Corte ha evidenziato come la sua compromissione incida non solo sulla sfera individuale, ma anche sull'architettura complessiva della sicurezza informatica. In particolare, la crittografia *end-to-end* è stata qualificata come una garanzia essenziale contro forme di sorveglianza indiscriminata, benché siano state riconosciute le difficoltà operative che essa può comportare per le autorità preposte all'applicazione della legge.

La Corte ha rilevato che l'imposizione ai fornitori di servizi di comunicazione dell'obbligo di fornire chiavi di decrittazione o di predisporre *backdoor* compromette la sicurezza dell'intera comunità degli utenti, e non soltanto quella dei soggetti sottoposti a indagine. Tali misure, infatti, aprono la strada a forme di sorveglianza generalizzata e indiscriminata, esponendo nel contempo le comunicazioni elettroniche a possibili abusi da parte di attori malevoli. In tale prospettiva, la Corte ha concluso che obblighi di questo tipo non possono essere considerati necessari in una società democratica.

Alla luce di tali considerazioni, la Corte ha sollecitato gli Stati a privilegiare strategie investigative selettive e proporzionate, evitando soluzioni che implichino un indebolimento sistemico della crittografia, con il conseguente rischio di compromettere la fiducia degli utenti nell'ecosistema digitale. La sentenza riafferma così la centralità della crittografia quale strumento imprescindibile per la tutela dei diritti fondamentali nell'era digitale.

9. Il First Report on Encryption *dell'*EU Innovation Lab *del 2024*

Infine, degno di nota è un rapporto recentissimo, intitolato *First Report on Encryption*, frutto della collaborazione tra alcune delle principali istituzioni europee impegnate nella sicurezza interna[23]. Il rapporto è stato realizzato dall'*EU Innovation Hub for Internal Security*, con il contributo di *Europol*, *Eurojust*, la Direzione Generale per la Migrazione e gli Affari Interni della Commissione Europea (DG HOME), il Centro Comune di Ricerca della Commissione Europea (JRC), il Coordinatore Europeo per l'Antiterrorismo e l'Agenzia Europea per la Gestione Operativa dei Sistemi IT su larga scala nell'Area di Libertà, Sicurezza e Giustizia (EU-LISA).

Questa collaborazione testimonia un approccio coordinato e multidisciplinare per affrontare i complessi problemi posti dalla crittografia in relazione alla sicurezza e alla giustizia. Il documento non si limita a descrivere la tensione tra sicurezza e *privacy*, ma analizza soluzioni concrete e scenari operativi, considerando le implicazioni legislative, tecnologiche e strategiche della crittografia. I contributi dei vari membri dell'*Innovation Hub* garantiscono una visione d'insieme che spazia dalle problematiche tecniche all'evoluzione delle normative nazionali e internazionali.

In particolare, il Rapporto analizza il crescente ruolo delle tecnologie emergenti, come la crittografia quantistica e i sistemi biometrici avanzati, oltre alle complessità introdotte da protocolli come il 5G e il RCS, che stanno trasformando il panorama delle comunicazioni digitali.

---

[23] EU INNOVATION HUB, *First Report on Encryption by the EU Innovation Hub for Internal Security*, Publications Office of the European Union, Luxembourg, 2024, in *https://www.europol.europa.eu/publications-events/publications/first-report-encryption*. Il rapporto analizza, tra l'altro, anche le misure proposte dalla Commissione Europea per contrastare il materiale pedopornografico online (CSAM), evidenziando un regolamento transitorio introdotto nel 2021. Questo è stato successivamente sostituito da una proposta legislativa del 2022 che mira a rafforzare gli obblighi di rilevamento attraverso l'utilizzo del *client-side scanning*. Quest'ultima è una tecnologia progettata per analizzare direttamente sul dispositivo dell'utente i contenuti presenti sui dispositivi degli utenti prima che vengano crittografati e inviati tramite sistemi di comunicazione protetti, come quelli che utilizzano crittografia *end-to-end*.

Tra i profili più rilevanti, il rapporto analizza le principali strategie adottate o discusse a livello governativo per ottenere accesso a dati cifrati. La prima consiste nell'imposizione di *backdoor*. Questa soluzione solleva per le su esposte ragioni evidenti criticità in termini di sicurezza informatica (vulnerabilità sistemiche sfruttabili anche da soggetti terzi non autorizzati). La seconda strategia si concentra sull'accesso ai dati nel momento antecedente alla loro cifratura, per esempio attraverso tecniche di intercettazione lato *client* o mediante strumenti installati sui dispositivi degli utenti. Sebbene formalmente meno invasiva rispetto alle *backdoor* generalizzate, anche questa opzione pone interrogativi significativi sul piano della proporzionalità e della compatibilità con il diritto al rispetto della vita privata e alla protezione dei dati personali.

Un esempio concreto dell'approccio innovativo adottato dai Paesi Bassi in materia di crittografia è rappresentato dall'introduzione dell'articolo 558 nel Codice di procedura penale, entrato in vigore il 1º ottobre 2022. Questa disposizione consente alle autorità di obbligare un sospettato a sbloccare un dispositivo sequestrato senza la necessità di ottenere il preventivo consenso di un giudice supervisore. La misura, definita come "coercizione proporzionata", amplia significativamente i poteri investigativi, pur essendo concepita come soluzione temporanea, soggetta a revisione dopo due anni[24].

Nel contesto di un dibattito sempre più acceso sulle capacità di accesso delle autorità ai dati digitali, il *Research and Documentation Centre* (WODC) olandese ha pubblicato il 31 agosto 2023 il rapporto *Police hacking regulation abroad*. Questo studio offre una prospettiva comparativa sulle normative e le garanzie legali relative all'intrusione nei sistemi informatici a fini investigativi, analizzando come diversi Paesi regolamentino tali strumenti. Il rapporto non si limita a descrivere le pratiche, ma fornisce spunti critici su come bilanciare efficacemente esigenze investigative e tutela dei diritti fondamentali. L'esperienza normativa dei Paesi Bassi, unita all'analisi comparativa condotta, evidenzia il loro ruolo di avanguardia nella ricerca di soluzioni equilibrate alle sfide poste dalla crittografia nelle indagini penali. Il rapporto com-

[24] V. p. 12 del Rapporto. Cfr. il testo della normativa olandese in *https://zoek.officielebekendmakingen.nl/stb-2022-276.html*.

plessivo sottolinea la necessità di bilanciare efficacemente la lotta alla criminalità con la tutela della *privacy* e della sicurezza informatica, promuovendo un dialogo inclusivo tra autorità pubbliche, settore tecnologico e società civile nel rispetto dei valori democratici.

GLI ELEMENTI DI PROVA GENERATI O RACCOLTI TRAMITE INTELLIGENZA ARTIFICIALE

CONSIDERAZIONI METODOLOGICHE

Luca Pressacco

SOMMARIO: *1. Processo penale e intelligenza artificiale: intersezioni. 2. La c.d. "prova algoritmica". 3. Intelligenza artificiale e prova penale: opportunità e rischi. 4. Le decisioni fondate su trattamenti automatizzati. 5. Intelligenza artificiale e "ciclo probatorio".*

1. Processo penale e intelligenza artificiale: intersezioni

Le tecnologie di intelligenza artificiale possono contribuire in vario modo all'esercizio della funzione giurisdizionale. In una prospettiva puramente gestionale, i *software* basati sull'intelligenza artificiale potrebbero essere impiegati per agevolare l'amministrazione degli uffici giudiziari e la distribuzione dei carichi di lavoro al loro interno. Gli strumenti in questione potrebbero, inoltre, rivelarsi utili per coadiuvare il giudice e i suoi ausiliari nelle attività d'udienza, a partire dalla redazione del verbale, oppure per la gestione e la consultazione dei fascicoli processuali, nonché per la traduzione degli atti in essi compresi[1].

A titolo esemplificativo, è possibile immaginare sistemi esperti che semplifichino il lavoro svolto dai funzionari giudiziari, estraendo auto-

[1] Per un inquadramento teorico di questi profili, v. G. UBERTIS, *Processo penale telematico, intelligenza artificiale e Costituzione*, in *Cass. pen.*, 2024, p. 439 ss. L'autore osserva che «il processo penale telematico non può in linea di principio riguardare lo svolgimento della forma processuale tipica, che è costituita dal dibattimento; questo è caratterizzato tra l'altro dai principi di immediatezza e di oralità, poco consoni (per dirla eufemisticamente) a una relazione unicamente tecnologica tra i protagonisti dell'evento processuale, ed è al più possibile che i suoi atti siano documentati (ma non compiuti) informaticamente».

maticamente dalla notizia di reato e inserendo nel relativo registro tutti i dati funzionali alle doverose iscrizioni[2], oppure ordinando e indicizzando gli atti e i documenti presenti all'interno dei fascicoli processuali.

Analogamente, per quanto riguarda l'esercizio della funzione giurisdizionale, sarebbero molto utili *software* progettati per calcolare i termini di prescrizione o di durata delle misure cautelari personali, nonché applicativi idonei ad assistere il giudice nell'impostazione e nella compilazione automatica della parte c.d. enunciativa dei provvedimenti giurisdizionali[3], senza trascurare le banche dati orientate alla ricerca giurisprudenziale. Si tratta di scenari indubbiamente promettenti, visto che le tecnologie in esame forniscono prestazioni eccellenti – di gran lunga superiori a quelle umane – quando si tratta di sintetizzare testi, compilare documenti standardizzati e svolgere attività ripetitive, basate sull'applicazione vincolata di regole logiche, matematiche o informatiche[4].

---

[2] Si rammenta che il registro delle notizie di reato è costituito, a sua volta, da un applicativo informatico: il c.d. *Re.Ge Web*, acronimo di Registro generale delle notizie di reato, che – unitamente al c.d. *BDMC* (Banca dati delle misure cautelari) – compone il c.d. *SICP*, vale a dire il Sistema informativo della cognizione penale.

[3] La parte enunciativa della sentenza, usualmente contrapposta a quella espositiva (ossia la motivazione) e a quella dispositiva (consistente nell'ordine del giudice), è composta: dall'intestazione del provvedimento, dall'indicazione dell'autorità giurisdizionale che lo ha pronunciato, dalle generalità dell'imputato e delle altri private (nonché dalle altre informazioni complementari concernenti, per esempio, il difensore e il domicilio), dall'imputazione e dall'indicazione delle richieste o conclusioni rassegnate dalle parti (cfr. l'art. 546, co. 1, lett. *a-d* c.p.p.). A ciò, nella prassi, si aggiunge sovente il riassunto per sommi capi dello svolgimento processuale, non previsto dalle disposizioni legislative, ma considerato utile per l'organizzazione razionale della motivazione.

[4] Persino un commentatore fortemente scettico nei confronti della penetrazione dell'intelligenza artificiale nel contesto processuale – poiché considerata sintomatica di una «nuova tendenza alla gestione economico-aziendalistica degli affari penali», che condurrà fatalmente a un distopico rito artificiale – è disposto ad ammettere che «il gigantismo digitale delle informazioni processuali renderà ineludibile l'impiego di sistemi algoritmici sempre più evoluti per la gestione di una mole di dati che supera le capacità umane»; riconoscendo in conclusione che, da questo punto di vista, la trasformazione digitale «presenta anche aspetti di segno positivo, in quanto le tecnologie, a regime, dovrebbero effettivamente semplificare alcune attività processuali»: O. MAZZA, *Distopia del processo artificiale*, in *Archivio penale* (rivista web) 7 gennaio 2025 (ultimo accesso il 28 febbraio 2025), da cui sono tratte le citazioni che precedono in nota (*ivi*, p. 2).

Ad ogni modo, se l'intelligenza artificiale entrerà nella prassi giudiziaria quotidiana, in che termini e con quali tempistiche dipenderà, in larga misura, dalle scelte (politiche, economiche, gestionali) compiute dalle autorità preposte all'organizzazione e al funzionamento dei servizi relativi alla giustizia (art. 110 Cost.), vale a dire in particolare dal Ministero della Giustizia e dal Consiglio superiore della Magistratura. Tali scelte, infatti, determineranno la propensione della pubblica amministrazione a investire nello sviluppo delle tecnologie in esame, promuovendone l'utilizzo anche nel settore giudiziario, storicamente refrattario alle innovazioni organizzative e tecnologiche[5].

In questa sede, tuttavia, non intendo soffermarmi su questi aspetti, che riguardano le applicazioni dirette dell'intelligenza artificiale in funzione di supporto alle variegate attività compiute dai soggetti processuali e, più in generale, dagli operatori coinvolti nel sistema di giustizia penale. L'intento, piuttosto, è quello di riflettere su una dimensione ulteriore di interferenza tra le nuove tecnologie e la giurisdizione penale. Mi riferisco, in particolare, all'ingresso sulla scena processuale di elementi di prova *generati*, *elaborati* o *raccolti* tramite *software* di *artificial intelligence*.

Questa intersezione, sebbene meno appariscente, non dovrebbe destare particolare stupore, visto che in dottrina è stato evidenziato a più riprese il nesso che intercorre tra il sistema probatorio processuale e l'orizzonte epistemologico (inteso come l'insieme delle pratiche conoscitive e delle credenze a esso associate) tipico di una determinata società[6]. Se dunque l'epoca contemporanea è caratterizzata da un prodigioso avanzamento delle tecnologie di intelligenza artificiale, che tendono a permeare ogni ambito della vita individuale e collettiva, allora è

[5] Per alcune considerazioni sul rapporto fra transizione digitale ed esercizio della funzione giurisdizionale, volendo, cfr. L. PRESSACCO, *Trasformazione digitale e funzione giurisdizionale*, in G. DI PAOLO (a cura di), *Trasformazioni della giustizia. Norme, organizzazione, tecnologie*, Napoli, 2024, p. 73 ss. Per un inquadramento generale dell'argomento, v. B. GALGANI, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, Milano, 2022, *passim*.

[6] Cfr., per tutti, F. CORDERO, *Il giudizio d'onore*, Milano, 1959, p. 68 ss.; M. TARUFFO, *La semplice verità. Il giudice e la costruzione dei fatti*, Roma, 2009, p. 4 ss.; G. UBERTIS, *Profili di epistemologia giudiziaria*, Milano, 2021, p. 4 ss.

agevole prevedere che anche il sistema probatorio subirà gli effetti di questa significativa transizione.

Ciò impone di svolgere alcune considerazioni introduttive sulla c.d. "prova algoritmica". Non si pretende, ovviamente, di esaurire una tematica che dischiude molteplici prospettive di indagine[7], bensì di svolgere alcune brevi considerazioni di carattere metodologico, in coerenza con gli obiettivi propri di un intervento programmato.

2. La c.d. "prova algoritmica"

Il primo quesito, che sorge spontaneo, inerisce all'inquadramento concettuale della c.d. "prova algoritmica". Si tratta di una nuova categoria dogmatica, meritevole di considerazione autonoma e foriera di una specifica disciplina giuridica? Ritengo che la risposta a questa domanda debba essere individuata, come per ogni questione categoriale, prestando attenzione alle ricadute operative della qualificazione in esame e saggiando la capacità esplicativa della stessa.

Da questo punto di vista, giova segnalare come le prospettive d'impiego dell'intelligenza artificiale nell'ambito del procedimento penale abbiano già sospinto il legislatore a introdurre talune definizioni autonome, delineando fattispecie assistite da specifiche garanzie procedurali.

Un esempio significativo, in questa direzione, è costituito dalla c.d. "profilazione", che l'art. 2 lett. *e* d.lgs. 18 maggio 2018 n. 51[8] definisce come

[7] In altra sede, per esempio, si è già indagato sul rapporto fra intelligenza artificiale e ragionamento probatorio, in prospettiva epistemologica: cfr., volendo, L. PRESSACCO, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, in *BioLaw Journal*, 2022, 4, p. 503 ss. (ora anche in G. DI PAOLO, L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Napoli, 2022, p. 91 ss.).

[8] Recante: «Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio».

> qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Consapevole della portata altamente invasiva dei trattamenti automatizzati orientati alla profilazione delle persone fisiche nella sfera della loro riservatezza, l'art. 8 del medesimo d.lgs. n. 51/2018 stabilisce che

> sono vietate le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge. Le disposizioni di legge devono prevedere garanzie adeguate per i diritti e le libertà dell'interessato. In ogni caso è garantito il diritto di ottenere l'intervento umano da parte del titolare del trattamento.

Si avrà modo di tornare in seguito su quest'ultima disposizione[9]. Per il momento, ciò che interessa mettere in luce è che il legislatore, consapevole dell'attitudine degli strumenti in questione a convertirsi in autentiche "tecnologie del controllo", idonee a conculcare le libertà individuali, ha avvertito l'esigenza di introdurre una regolazione specifica per talune sue particolari applicazioni.

Ciò non toglie, tuttavia, che la prova generata o raccolta tramite strumenti di intelligenza artificiale possa essere utilmente ricondotta entro il *genus* della prova scientifica e, in particolare, nel novero della c.d. prova digitale o informatica[10]. L'inquadramento dogmatico risulta proficuo poiché identifica gli snodi concettuali che non possono essere pretermessi nelle diverse fasi del procedimento probatorio, qualora vengano in rilievo elementi di prova siffatti.

---

[9] V. *infra*, par. 4.

[10] Nel medesimo senso, v. M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, p. 61 ss.

Così, quale che sia il canale prediletto per l'inserimento della prova algoritmica nel processo penale[11], la decisione sull'ammissione della prova non potrà mai prescindere dalla considerazione delle leggi scientifiche sottese al funzionamento dell'algoritmo, pena il rischio di introdurre nel contesto processuale informazioni irrilevanti (in quanto basate su fondamenta scientifiche non attendibili in linea di principio o non adeguate all'applicazione prevista).

Analogamente, nella fase di assunzione della prova, occorrerà tenere conto delle caratteristiche tipiche della *electronic evidence* come, per esempio, l'immaterialità, la congenita modificabilità e la promiscuità delle informazioni generate o raccolte tramite l'intelligenza artificiale.

Infine, la natura della "prova algoritmica" (eventualmente ammessa) emergerà nuovamente al momento della sua valutazione, quando si tratterà di individuarne l'effettiva persuasività, tenendo conto altresì del margine di errore insito nello strumento considerato.

3. Intelligenza artificiale e prova penale: opportunità e rischi

Allo stadio attuale, due sono i principali punti di intersezione tra la prova penale e l'intelligenza artificiale[12].

Il primo è costituito dalla c.d. "automatedly generated evidence"[13]. Si tratta delle informazioni generate automaticamente, prevalentemente

[11] Cfr., sul punto, S. QUATTROCOLO, *L'ammissione della prova alla luce della rivoluzione digitale*, in E.M. CATALANO, P. FERRUA (a cura di), *Corderiana. Sulle orme di un maestro del rito penale*, Torino, 2023, p. 163 ss.; G. UBERTIS, *Perizia, prova scientifica e intelligenza artificiale nel processo penale*, in S. PATTI, R. POLI, *La consulenza tecnica d'ufficio. Funzione, oggetto, sindacabilità*, Torino, 2024, p. 181 ss. In termini generali, v. anche M. CAIANIELLO, *L'ammissione della prova scientifica nel processo penale italiano*, in G. CANZIO, L. LUPARIA DONATI (a cura di), *Prova scientifica e processo penale*, Milano, 2022, p. 189 ss.

[12] Cfr., al riguardo, K. LIGETI, *AI Evidence: Ensuring a Fair Trial in the Digital World*, in M. BERGSTRÖM, V. MITSILEGAS (eds.), *EU Law in the Digital Age*, Oxford-Dublin, 2025, p. 225 ss.

[13] Per una compiuta elaborazione della categoria della "prova generata automaticamente" v., da ultima, S. QUATTROCOLO, *Prova e intelligenza artificiale*, in C. CONTI, A. MARANDOLA (a cura di), *La prova scientifica*, Milano, 2023, p. 467 ss.

per motivi commerciali, da prodotti di consumo che utilizzano o applicano strumenti di intelligenza artificiale. Si pensi, a titolo puramente esemplificativo, alle informazioni incamerate dai sistemi di guida assistita presenti all'interno degli autoveicoli tecnologicamente avanzati, ai dati registrati dai dispositivi integrati in una rete domotica (nella quale possono rientrare anche sistemi di sorveglianza) oppure, ancora, alle informazioni registrate da alcune applicazioni per il monitoraggio dei parametri corporei presenti nei dispositivi elettronici mobili. Questi dati, ovviamente, costituiscono un vasto patrimonio informativo, potenzialmente rilevante anche nell'ambito di un procedimento penale.

Il secondo profilo da tenere in considerazione è costituito dai sistemi di analisi forense che integrano *software* di intelligenza artificiale per lo svolgimento dei relativi esami. Si pensi, in particolare, ai sistemi di riconoscimento facciale – e di analisi biometrica in generale[14] –, oppure ai *software* di analisi documentale, che consentono di filtrare ed esaminare una vastissima congerie di *file* digitali.

Entrambe le applicazioni considerate rappresentano una preziosa opportunità per il sistema di giustizia penale, ma sollevano anche numerosi interrogativi a causa dei rischi che si intravedono nella loro implementazione pratica.

Per quanto riguarda le informazioni generate automaticamente, occorre tenere sempre presente che i *software* da cui risultano prodotte sono stati progettati e realizzati per finalità differenti rispetto a quelle propriamente processuali. Ciò genera il rischio di un utilizzo improprio dei dati in esame e la produzione di gravi fraintendimenti cagionati dal c.d. *function creep*, che si verifica quando una certa tecnologia viene utilizzata al di fuori del dominio e degli scopi per cui è stata originariamente creata[15]. Si rende dunque necessaria una verifica accurata circa l'autenticità e l'attendibilità dell'informazione estratta dai singoli dispositivi per non incappare in errori che si rivelano fatali nella ricostruzione dei fatti in sede giudiziale[16].

---

[14] Su cui v. E. SACCHETTO, *La prova biometrica*, in C. CONTI, A. MARANDOLA (a cura di), *La prova scientifica*, cit., p. 243 ss.

[15] K. LIGETI, *AI Evidence: Ensuring a Fair Trial in the Digital World*, cit., p. 233.

[16] S. QUATTROCOLO, *Prova e intelligenza artificiale*, cit., p. 493.

Le difficoltà, com'è agevole intuire, sono legate alla necessità di verificare compiutamente il funzionamento del sistema di intelligenza artificiale che ha generato quell'informazione: ciò richiederebbe, infatti, di avere pieno accesso all'algoritmo proprietario, così come ai dati di addestramento del *software*.

Una tale situazione di completezza informativa sembra di difficile realizzazione, data l'esigenza di tutelare la riservatezza delle creazioni coperte da privativa industriale, senza che si possa rimproverare alle imprese produttrici la mancata cooperazione con l'autorità giudiziaria (dal momento che si troverebbero involontariamente coinvolte nella vicenda processuale). Di conseguenza, ove il legislatore non si premuri di introdurre un meccanismo specifico di *disclosure* controllata per affrontare le situazioni di questo genere, l'interprete si troverebbe di fronte a una rigida alternativa: l'esclusione in radice delle informazioni in questione dal contesto processuale (non essendo possibile verificarne autenticità, attendibilità e precisione) o la loro fideistica ammissione.

Ovviamente, nessuna delle due soluzioni appare pienamente soddisfacente. Una via mediana sembra, tuttavia, percorribile adottando un approccio pragmatico. In effetti, potrebbe apparire eccessivo escludere dalla scena processuale determinate informazioni solo perché derivano da certe tecnologie, magari già ampiamente sperimentate e utilizzate nella vita quotidiana.

Per intenderci, una volta acquisito lo scontrino emesso dalla cassa automatica collocata all'interno di un supermercato, sembra difficile ipotizzare che il giudice disponga una minuziosa perizia per sviscerare tutti i meccanismi elettronici e informatici che ne regolano il funzionamento, a meno che non vi siano serie contestazioni in merito alle modalità di fatturazione o alla determinazione dell'orario di emissione della ricevuta (magari con la produzione delle tanto temute "allucinazioni").

Analogamente, non è detto che l'ammissione in giudizio di determinati elementi di prova debba essere subordinato alla disponibilità di informazioni specifiche e dettagliate sui sistemi di *artificial intelligence* che li hanno prodotti, ferma restando la necessità di mettere a disposizione di tutte le parti il *data-set* estratto dal dispositivo in questione.

Qualora, poi, l'attendibilità di questi dati fosse posta in discussione, il giudice avrebbe il dovere di valutare la necessità di disporre una peri-

zia o un esperimento giudiziario per verificare l'effettivo funzionamento del sistema, eventualmente attraverso un approccio di *reverse engineering*. Per converso, senza pieno accesso al *data-set* estratto dal dispositivo diviene impossibile garantire la parità delle armi e il diritto al "confronto" con la prova algoritmica, come ha posto in luce la dottrina più sensibile al tema[17]. Difatti, non sarebbe possibile verificare se le informazioni raccolte siano idonee, per quantità e qualità, a soddisfare le esigenze di accertamento dei fatti, né sarebbe possibile operare su di esse per ricostruire *ex post* la logica del sistema che le ha generate.

Problematiche solo in parte analoghe si riscontrano in relazione ai *Forensic Tools* che si avvalgono dell'intelligenza artificiale per lo svolgimento di esami ed analisi. Questi ultimi, infatti, sono progettati per le finalità tipiche del procedimento penale e dovrebbero garantire elevati standard di qualità. Inoltre, i *software* in questione sono spesso sviluppati direttamente dalle agenzie di *law enforcement* o, comunque, su impulso di un committente pubblico, motivo per cui le imprese produttrici non potrebbero dolersi di essere rimaste casualmente coinvolte nei procedimenti penali in cui quegli strumenti hanno trovato impiego[18].

Con l'introduzione del c.d. *Artificial Intelligence Act*[19], gli strumenti in questione hanno conosciuto una prima forma di regolazione. Difatti, tutti i sistemi volti alla valutazione di affidabilità di elementi probatori (nella fase delle indagini) e quelli volti alla ricerca e alla interpretazione

[17] E. BAMPASIKA, *AI-Based Means of Evidence and the Defendant's Right in the European Union*, in M. BERGSTRÖM, V. MITSILEGAS (eds.), *EU Law in the Digital Age*, cit., p. 247 ss.

[18] Cfr., *mutatis mutandis*, Cons. St., sent. sentenza 4 febbraio 2020 n. 881, § 10, ove si è affermato perentoriamente che «la caratterizzazione multidisciplinare dell'algoritmo (costruzione che certo non richiede solo competenze giuridiche, ma tecniche, informatiche, statistiche, amministrative) non esime dalla necessità che la 'formula tecnica', che di fatto rappresenta l'algoritmo, sia corredata da spiegazioni che la traducano nella "regola giuridica" a essa sottesa e che la rendano leggibile e comprensibile»; precisando, inoltre, che «non può assumere rilievo [in senso contrario] l'invocata riservatezza delle imprese produttrici dei meccanismi informatici utilizzati i quali, ponendo al servizio del potere autoritativo tali strumenti, all'evidenza ne accettano le relative conseguenze in termini di necessaria trasparenza».

[19] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale.

dei fatti rilevanti (in sede di giudizio) sono considerati come applicazioni ad alto rischio, ai sensi dell'allegato III del medesimo regolamento europeo, cui rinvia l'art. 6 § 2 Reg. (UE) 1689/2024. Ciò implica che essi debbano sottostare a tutte le cautele e agli obblighi di trasparenza, qualità e vigilanza disciplinati dal regolamento in esame di cui, tuttavia, sono ben noti inconvenienti ed eccezioni. In particolare, per quanto riguarda i *software* di analisi forense, è legittimo domandarsi se sia possibile "evadere" dalla stringente disciplina dettata per i sistemi ad alto rischio, facendo leva sulle clausole di salvaguardia contenute nell'art. 6 § 3 Reg. (UE) 1689/2024[20]. È chiaro, infatti, che, se queste disposizioni fossero interpretate in senso lato, gran parte dei dispositivi di analisi forense potrebbe essere escluso dal novero dei sistemi ad alto rischio, con un significativo abbassamento degli standard di trasparenza e di qualità previsti per questi ultimi[21].

Sarebbe un esito davvero beffardo e poco auspicabile. In tal caso, difatti, per rispettare l'equità processuale e la parità delle armi, non resterebbe che affidarsi alle scarne – benché meritevoli di apprezzamento – indicazioni giurisprudenziali emerse fino a questo momento.

Muovendo dalle statuizioni più recenti, nelle pronunce sui c.d. criptofonini, la Corte di Cassazione ha espressamente riconosciuto che, in linea di principio, «la disponibilità dell'algoritmo di criptazione è funzionale al controllo dell'affidabilità del contenuto delle comunicazioni acquisite al procedimento»[22].

---

[20] Laddove si esclude che i sistemi di cui all'allegato III debbano essere considerati ad alto rischio quando siano destinati: a) a eseguire un *compito procedurale limitato*; b) a migliorare il risultato di un'attività umana precedentemente completata; c) a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non siano finalizzati a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; d) a eseguire un *compito preparatorio* per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III.

[21] Cfr., sulle eccezioni in esame, T. RODRÌGUEZ DE LAS HERAS BALLEL, *High-Risk AI Systems in the European AI Act*, in O. POLLICINO et al. (a cura di), *La disciplina dell'intelligenza artificiale*, Milano, 2025, p. 241 ss.

[22] Cass., sez. un., sent. 29 febbraio 2024 n. 23755, Gjuzi Ermal, § 12.4, in *CED Cass.*, n. 286573 – 06 (ove, peraltro, la conseguenza logica di tale statuizione di massima è stata "sterilizzata", considerando che «il pericolo di alterazione dei dati non sussiste, salvo specifiche allegazioni di segno contrario, in quanto il contenuto di ciascun

La Corte di Strasburgo, dal canto suo, ha stabilito da tempo che – ove le autorità inquirenti abbiano effettuato il sequestro di una vasta mole di prove digitali, filtrate in seguito attraverso strumenti informatici di analisi documentale – tali *software* dovrebbero essere posti anche a disposizione della difesa, nella misura in cui si rivelino utili a garantire le facilitazioni necessarie per l'esercizio del diritto di difesa, ai sensi dell'art. 6 § 3 lett. *b* Cedu[23].

4. Le decisioni fondate su trattamenti automatizzati

Venendo, infine, al versante propriamente decisionale, giova soffermarsi rapidamente sul già menzionato art. 8 del d.lgs. n. 51/2018. Senza voler indugiare troppo su una disposizione che ha suscitato notevole attenzione in dottrina per il suo significato (anche simbolico) di garanzia, giova segnalare alcune questioni esegetiche problematiche, utili per individuare la portata delle garanzie legislative.

Anzitutto, sebbene talvolta venga intesa come un divieto assoluto di impiegare decisioni automatizzate nel contesto processuale, dal tenore letterale della disposizione si comprende agevolmente come, in realtà, l'interdizione sia soltanto relativa, essendo ancorata al rispetto della riserva di legge (europea o nazionale)[24].

Nei casi in cui la riserva di legge venga attuata e, di conseguenza, l'impiego di decisioni automatizzate sia stato debitamente autorizzato, il legislatore è chiamato a garantire i diritti e le libertà dei soggetti interessati tramite apposite garanzie procedurali. Fra queste ultime spicca, in particolare, il diritto a ottenere un controllo umano da parte del titola-

---

messaggio è inscindibilmente abbinato alla sua chiave di cifratura, per cui una chiave errata non ha alcuna possibilità di decriptarlo, anche solo parzialmente»).

[23] Corte eur. dir. uomo, sent. 4 giugno 2019, Sigurdur Einarsson e altri c. Islanda, § 90-91. Per gli opportuni approfondimenti al riguardo, cfr. L. BARTOLI, *Parità delle armi e* e-discovery *nel processo penale: quali indicazioni da Strasburgo?*, in R. BRIGHI (a cura di), *Nuove questioni di informatica forense*, Roma, 2022, p. 83 ss.

[24] In tal senso, v. L. LUPARIA, *Diritto probatorio e giudizi criminali ai tempi dell'intelligenza artificiale*, in R. GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano, 2022, p. 782.

re del trattamento, che deve essere assicurato in ogni caso dalla pertinente normativa[25].

In secondo luogo, sempre facendo riferimento al dato testuale, si evince con sufficiente chiarezza che il divieto in esame – nei termini in cui è stato ricostruito in precedenza – non riguarda soltanto l'adozione di decisioni giurisdizionali tramite programmi automatizzati (il c.d. giudice-robot), ma anche l'emissione di decisioni che siano basate in modo esclusivo o determinate sugli elementi generati da un trattamento automatizzato di dati. Se così non fosse, non si comprenderebbe lo specifico riferimento alla profilazione, che costituisce senza dubbio un trattamento automatizzato di dati, posto a supporto di un processo decisionale più ampio. Nel disegno normativo, dunque, l'emissione del provvedimento costituisce un'entità concettualmente distinta – e logicamente successiva – rispetto al trattamento di dati personali, su cui la decisione risulta fondata[26].

Infine, giova precisare che il divieto sancito dalla norma in esame colpisce soltanto i trattamenti automatizzati che producono *effetti pregiudizievoli* nei confronti degli interessati. Rimane, dunque, insoluto il quesito ermeneutico su quali sarebbero le conseguenze giuridiche nell'ipotesi in cui un trattamento automatizzato producesse, al contrario, effetti potenzialmente favorevoli per i soggetti interessati. È evidente

[25] Per una critica a tale impostazione legislativa, v. S. SIGNORATO, *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati: un nuovo diritto derivante dal rispetto della dignità umana*, in *Riv. dir. process.*, 2021, pp. 107 ss., ove si sostiene che la decisione algoritmica sia radicalmente incompatibile con il diritto al rispetto della dignità umana e che «tale violazione non potrebbe ritenersi sanata dal successivo (oltretutto eventuale) intervento umano» (*ivi*, p. 108). Di conseguenza, l'autrice dubita «della legittimità dell'art. 11 dir. 2016/680/UE e dell'art. 8 d.lgs. 18 maggio 2018 n. 51 nella parte in cui essi prevedono che la decisione robotica possa essere autorizzata dal diritto dell'Unione o degli Stati membri» (*ivi*, p. 109).

[26] Muovendo da queste considerazioni, si giunge ad affermare che la disposizione in commento non si limita a vietare l'emissione (*rectius*: la deliberazione) di provvedimenti giurisdizionali tramite strumenti di IA, ma prescrive anche una regola negativa di valutazione della prova, analoga a quella prevista dall'art. 192, co. 2 c.p.p. In questa direzione, v. M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Diritto penale contemporaneo - Archivio web*, 29 maggio 2019, p. 17 (ultimo accesso il 28 febbraio 2025).

che, qualora si ritenesse necessario verificare la concreta incidenza delle informazioni generate o elaborate mediante un trattamento automatizzato, l'interdizione prevista dall'art. 8 d.lgs. n. 51/2018 dovrebbe essere concepita alla stregua di un vero e proprio criterio di valutazione della prova[27].

5. Intelligenza artificiale e "ciclo probatorio"

Un'ultima considerazione in merito al contesto in cui è destinato a svilupparsi il dibattito sugli elementi di prova generati o raccolti tramite strumenti di intelligenza artificiale.

In dottrina è stato evidenziato come, a dispetto delle regole che disciplinano l'ammissione della prova in giudizio in ciascun ordinamento, ogni "nuovo" strumento di prova, frutto dell'evoluzione della scienza o della tecnica, attraversa un "ciclo probatorio"[28] nel quale sono riconoscibili – approssimativamente – i seguenti stadi (senza che tra essi siano sempre individuabili rigide separazioni o che il passaggio da uno stadio all'altro sia irreversibile):

a) Too new to be reliable
b) New but subject to testing
c) Generally reliable but occasionally improperly applied
d) Blindly Trusted.

Ciò costituisce ulteriore riprova del legame profondo che intercorre tra il sistema probatorio processuale e l'orizzonte epistemologico di riferimento in una determinata epoca storica. Se, come appare probabi-

[27] Sembra riproporsi, sotto nuove sembianze, l'antica diatriba dottrinale sull'efficacia delle prove illegittimamente acquisite, le quali sarebbero inutilizzabili *contra reum*, mentre – secondo parte della dottrina – potrebbero essere oggetto di valutazione in favore dell'imputato (cfr., al riguardo, F. CORDERO, *Prove illecite* (1961), in ID., *Tre studi sulle prove penali*, Milano, 1963, p. 171, il cui pensiero è stato ripreso, recentemente, da F. CAPRIOLI, *Verità e giustificazione nel processo penale*, in G. FORTI, G. VARRASO, M. CAPUTO (a cura di), *«Verità» del precetto e della sanzione alla prova del processo*, Napoli, 2014, pp. 204-205, ricordando che «l'accertamento dell'innocenza è una posta troppo importante, per essere sacrificata agli idoli della procedura»).

[28] V. S. GLESS, *AI in the Courtroom: a Comparative Analysis of Machine Evidence in Criminal Trials*, in 51 *Georgetown Journal of International Law* (2020), no. 2, p. 195 ss.

le, anche gli elementi di prova generati o raccolti tramite l'intelligenza artificiale sono destinati ad affrontare queste evoluzioni ed involuzioni, è opportuno cominciare ad attrezzarsi culturalmente e giuridicamente, affinché l'interprete – sia esso pubblico ministero, avvocato o giudice – sia davvero artefice consapevole delle proprie decisioni e non rimanga esposto alle intemperie, in balia dalla corrente.

SSM
Scuola Superiore della Magistratura

Struttura Didattica Territoriale Distretto della Corte di Appello di Trento

UNIVERSITÀ DI TRENTO
Facoltà di Giurisprudenza

2023-2027
DIPARTIMENTO DI ECCELLENZA
MUR

Convegno
Indagini e prove nella società digitale. Questioni attuali e prospettive future

Trento, 26- 27 settembre 2024

26 settembre (14.30-19.00)

14.30 Saluti istituzionali

Comunicazioni digitali e prova penale

14.45 Presiede, Introduce e Modera: Prof.ssa Gabriella Di Paolo, Università di Trento

15.00 I confini mobili delle intercettazioni - **Prof. Alberto Camon, Università di Bologna**

15.30 Comunicazioni criptate e prova penale: alla ricerca di nuovi paradigmi – **Prof.ssa Donatella Curtotti, Università di Foggia**

16.00 I dati esterni delle comunicazioni: tendenze evolutive - **Dott.ssa Federica Iovene, Procura della Repubblica di Bolzano**

16.30 Pausa

Circolazione probatoria interna e transfrontaliera

Presiede, Introduce e Modera: prof. Giulio Illuminati, Università di Bologna

17.00 La circolazione degli esiti delle intercettazioni in altri procedimenti interni - **dott. Luigi Giordano, Procura Generale della Corte di Cassazione**

17.30 L'acquisizione transfrontaliera di prove digitali **– Prof.ssa Rosanna Belfiore, Università di Catania**

18.00 Intervento programmato:

Intercettazioni e terzi estranei al procedimento. Corte Edu, Contrada c. Italia, 23 maggio 2023 - **dott.ssa Marianna Biral, Università di Trento**

Dibattito

19.00 Sospensione dei lavori

27 settembre (9.00-13.00)

Indagini tecnologicamente assistite e tecniche investigative speciali

9.15 Presiede, Introduce e Modera: prof. Fabio Salvatore Cassibba, Università di Parma

9.30 I Sequestri di smartphone, dispositivi informatici e memorie digitali – **Prof.ssa Elisa Lorenzetto, Università di Verona**

10.00 La geolocalizzazione: tecniche e garanzie – **Prof.ssa Silvia Signorato, Università di Padova**

10.30 Pausa

11.00 Operazioni sotto copertura nella rete – **Prof. Pasquale Bronzo, Università di Roma La Sapienza**

11.30 Indagini penali e criptovalute **– prof. Jacopo Della Torre, Università di Genova,**

12.00 Interventi programmati:

Backdoor nei sistemi crittografici e diritti umani – **prof. Antonino Ali – Università di Trento e De Cifris**

La valutazione degli elementi di prova generati o raccolti tramite intelligenza artificiale - **dott. Luca Pressacco, Università di Trento**

Dibattito

13.15 Chiusura dei lavori

Comitato Scientifico: Prof.ssa Gabriella Di Paolo, dott. Luca Pressacco

L'evento è stato organizzato dalla Facoltà di Giurisprudenza dell'Università di Trento nell'ambito del Dipartimento d'Eccellenza, in collaborazione con la SSM, Struttura Didattica Territoriale del Distretto di Corte d'Appello di Trento, con il Patrocinio della Camera Penale di Trento "Michele Pompermaier" e dell'Associazione Italiana Studiosi della Prova (AISP).
L'evento è accreditato presso l'Ordine degli Avvocati di Trento e Rovereto. Per ulteriori informazioni sul contenuto dell'evento e la registrazione, si rinvia alla pagina web: **https://webmagazine.unitn.it/evento/giurisprudenza/121210/indagini-e-prove-nella-societ-digita**

AISP
Associazione Italiana Studiosi della Prova

CAMERA PENALE TRENTO

COLLANA
'QUADERNI DELLA FACOLTÀ DI GIURISPRUDENZA'

UNIVERSITÀ DEGLI STUDI DI TRENTO

1. *L'applicazione delle regole di concorrenza in Italia e nell'Unione europea. Atti del IV Convegno Antitrust tenutosi presso la Facoltà di Giurisprudenza dell'Università di Trento* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE CARPAGNANO (2014)

2. *Dallo status di cittadino ai diritti di cittadinanza* - (a cura di) FULVIO CORTESE, GIANNI SANTUCCI, ANNA SIMONATI (2014)

3. *Il riconoscimento dei diritti storici negli ordinamenti costituzionali* - (a cura di) MATTEO COSULICH, GIANCARLO ROLLA (2014)

4. *Il diritto del lavoro tra decentramento e ricentralizzazione. Il modello trentino nello spazio giuridico europeo* - (a cura di) ALBERTO MATTEI (2014)

5. *European Criminal Justice in the Post-Lisbon Area of Freedom, Security and Justice* - JOHN A.E. VERVAELE, with a prologue by Gabriele Fornasari and Daria Sartori (Eds.) (2014)

6. *I beni comuni digitali. Valorizzazione delle informazioni pubbliche in Trentino* - (a cura di) ANDREA PRADI, ANDREA ROSSATO (2014)

7. *Diplomatici in azione. Aspetti giuridici e politici della prassi diplomatica nel mondo contemporaneo* - (a cura di) STEFANO BALDI, GIUSEPPE NESI (2015)

8. *Il coordinamento dei meccanismi di stabilità finanziaria nelle Regioni a Statuto speciale* - (a cura di) ROBERTO TONIATTI, FLAVIO GUELLA (2014)

9. *Reti di libertà. Wireless Community Networks: un'analisi interdisciplinare* - (a cura di) ROBERTO CASO, FEDERICA GIOVANELLA (2015)

10. *Studies on Argumentation and Legal Philosophy. Further Steps Towards a Pluralistic Approach* - (Ed. by) MAURIZIO MANZIN, FEDERICO PUPPO, SERENA TOMASI (2015)

11. *L'eccezione nel diritto. Atti della giornata di studio (Trento, 31 ottobre 2013)* - (a cura di) SERGIO BONINI, LUCIA BUSATTA, ILARIA MARCHI (2015)

12. José Luis Guzmán D'Albora, *Elementi di filosofia giuridico-penale* - (a cura di) GABRIELE FORNASARI, ALESSANDRA MACILLO (2015)

13. *Verso nuovi rimedi amministrativi? Modelli giustiziali a confronto* - (a cura di) GIANDOMENICO FALCON, BARBARA MARCHETTI (2015)

14. *Convergences and Divergences between the Italian and the Brazilian Legal Systems* - (Ed. by) GIUSEPPE BELLANTUONO, FEDERICO PUPPO (2015) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle. net/11572/116513)

15. *La persecuzione dei crimini internazionali. Una riflessione sui diversi meccanismi di risposta. Atti del XLII Seminario internazionale di studi italo-tedeschi, Merano 14-15 novembre 2014 - Die Verfolgung der internationalen Verbrechen. Eine Überlegung zu den verschiedenen Reaktionsmechanismen. Akten des XLII. Internationalen Seminars deutsch-italienischer Studien, Meran 14.-15. November 2014* - (a cura di / herausgegeben von) ROBERTO WENIN, GABRIELE FORNASARI, EMANUELA FRONZA (2015)

16. *Luigi Ferrari Bravo. Il diritto internazionale come professione* - (a cura di) GIUSEPPE NESI, PIETRO GARGIULO (2015)

17. *Pensare il diritto pubblico. Liber Amicorum per Giandomenico Falcon* - (a cura di) MAURIZIO MALO, BARBARA MARCHETTI, DARIA DE PRETIS (2015)

18. *L'applicazione delle regole di concorrenza in Italia e nell'Unione europea. Atti del V Convegno biennale Antitrust. Trento, 16-18 aprile 2015* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE CARPAGNANO (2015)

19. *From Contract to Registration. An Overview of the Transfer of Immoveable Property in Europe* - (Ed. by) ANDREA PRADI (2015) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle. net/11572/140085)

20. *Diplomatici in azione. Aspetti giuridici e politici della prassi diplomatica nel mondo contemporaneo. Volume II* - (a cura di) STEFANO BALDI, GIUSEPPE NESI (2016) (pubblicazione disponibile solo on-line in Accesso Aperto: http:// hdl.handle.net/11572/143369)

21. *Democrazie e religioni: libertà religiosa, diversità e convivenza nell'Europa del XXI secolo. Atti del convegno nazionale Adec Trento, 22 e 23 ottobre 2015* - (a cura di) ERMINIA CAMASSA (2016)

22. *Modelli di disciplina dell'accoglienza nell'"emergenza immigrazione". La situazione dei richiedenti asilo dal diritto internazionale a quello regionale* - (a cura di) JENS WOELK, FLAVIO GUELLA, GRACY PELACANI (2016)

23. *Prendersi cura dei beni comuni per uscire dalla crisi. Nuove risorse e nuovi modelli di amministrazione* - (a cura di) MARCO BOMBARDELLI (2016)

24. *Il declino della distinzione tra diritto pubblico e diritto privato. Atti del IV Congresso nazionale SIRD. Trento, 24-26 settembre 2015* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE GRAZIADEI (2016)

25. Fiat Intabulatio. *Studi in materia di diritto tavolare con una raccolta di normativa* - (a cura di) ANDREA NICOLUSSI, GIANNI SANTUCCI (2016)

26. *Le definizioni nel diritto. Atti delle giornate di studio, 30-31 ottobre 2015* - (a cura di) FULVIO CORTESE, MARTA TOMASI (2016)

27. *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali. Atti del convegno. Trento, 2 e 3 ottobre 2015* - (a cura di) ROBERTO WENIN, GABRIELE FORNASARI (2017)

28. *Studies on Argumentation & Legal Philosophy / 2. Multimodality and Reasonableness in Judicial Rhetoric* - (Ed. by) MAURIZIO MANZIN, FEDERICO PUPPO, SERENA TOMASI (2017) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/106571)

29. *Il Giudice di pace e la riforma della magistratura onoraria. Atti del Convegno. Trento, 3-4 dicembre 2015* - (a cura di) GABRIELE FORNASARI, ELENA MATTEVI (2017) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl. handle.net/11572/178978)

30. *Il diritto in migrazione. Studi sull'integrazione giuridica degli stranieri* - (a cura di) FULVIO CORTESE, GRACY PELACANI (2017)

31. *Diplomatici in azione. Aspetti giuridici e politici della prassi diplomatica nel mondo contemporaneo. Volume III* - (a cura di) STEFANO BALDI, GIUSEPPE NESI (2017) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/184772)

32. *Carlo Beduschi. Scritti scelti* - (a cura di) LUCA NOGLER, GIANNI SANTUCCI (2017)

33. *Diplomatici. 33 saggi su aspetti giuridici e politici della diplomazia contemporanea* - (a cura di) STEFANO BALDI, GIUSEPPE NESI (2018)

34. *Sport e fisco* - (a cura di) ALESSANDRA MAGLIARO (2018)

35. *Legal Conversations Between Italy and Brazil* - (a cura di) GIUSEPPE BELLANTUONO, FABIANO LARA (2018)

36. *Studies on Argumentation & Legal Philosophy / 3. Multimodal Argumentation, Pluralism and Images in Law* - (Ed. by) MAURIZIO MANZIN, FEDERICO PUPPO, SERENA TOMASI (2018) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/218719)

37. *Assetti istituzionali e prospettive applicative del* private antitrust enforcement *nell'Unione europea. Atti del VI convegno biennale antitrust. Facoltà di Giurisprudenza. Trento, 6-8 aprile 2017* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE CARPAGNANO (2018)

38. *La Direttiva quadro sulle acque (2000/60/CE) e la Direttiva alluvioni (2007/60/CE) dell'Unione europea. Attuazione e interazioni con particolare riferimento all'Italia* - (a cura di) MARIACHIARA ALBERTON, MARCO PERTILE, PAOLO TURRINI (2018)

39. *Saggi di diritto economico e commerciale cinese* - (a cura di) IGNAZIO CASTELLUCCI (2019)

40. *Giustizia riparativa. Responsabilità, partecipazione, riparazione* - (a cura di) GABRIELE FORNASARI, ELENA MATTEVI (2019) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/ 11572/234755)

41. *Prevenzione dei sinistri in area valanghiva. Attività sportive, aspetti normativo-regolamentari e gestione del rischio* - (a cura di) ALESSANDRO MELCHIONDA, STEFANIA ROSSI (2019)

42. *Pubblica amministrazione e terzo settore. Confini e potenzialità dei nuovi strumenti di collaborazione e sostegno pubblico* - (a cura di) SILVIA PELLIZZARI, ANDREA MAGLIARI (2019)

43. *Il private antitrust enforcement in Italia e nell'Unione europea: scenari applicativi e le prospettive del mercato. Atti del VII Convegno Antitrust di Trento, 11-13 aprile 2019* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE CARPAGNANO (2019)

44. *Conciliazione, mediazione e deflazione nel procedimento davanti al giudice di pace. Esperienze euroregionali. Atti del Convegno. Trento, 10 maggio 2019* - (a cura di) SILVANA DALLA BONTÀ, ELENA MATTEVI (2020) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/ 259285)

45. *Diritto e genere. Temi e questioni* - (a cura di) STEFANIA SCARPONI (2020)

46. *Le parti in mediazione: strumenti e tecniche. Dall'esperienza pratica alla costruzione di un metodo* - (a cura di) SILVANA DALLA BONTÀ (2020) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572 /269082)

47. *Effettività delle tutele e diritto europeo. Un percorso di ricerca per e con la formazione giudiziaria* - (a cura di) PAOLA IAMICELI (2020)

48. *Infermità mentale, imputabilità e disagio psichico in carcere. Definizioni, accertamento e risposte del sistema penale* - (a cura di) ANTONIA MENGHINI, ELENA MATTEVI (2020)

49. *Le (in)certezze del diritto. Atti delle giornate di studio. 17-18 gennaio 2019* - (a cura di) CINZIA PICIOCCHI, MARTA FASAN, CARLA MARIA REALE (2021)

50. *Studies on Argumentation & Legal Philosophy / 4. Ragioni ed emozioni nella decisione giudiziale* - (Ed. by) MAURIZIO MANZIN, FEDERICO PUPPO, SERENA TOMASI (2021) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl.handle.net/11572/296052)

51. *Comunicare, negoziare e mediare in rete. Atti del Convegno. Trento, 25 settembre 2020* - (a cura di) SILVANA DALLA BONTÀ (2021) (pubblicazione disponibile solo on-line in Accesso Aperto: http://hdl. handle.net/11572/306972)

52. *La giurisdizione penale del giudice di pace: un bilancio sui primi vent'anni* - (a cura di) MARCELLO BUSETTO, GABRIELLA DI PAOLO, GABRIELE FORNASARI, ELENA MATTEVI (2021)

53. *State and Religion: Agreements, Conventions and Statutes* - (Ed. by) CINZIA PICIOCCHI, DAVIDE STRAZZARI, ROBERTO TONIATTI (2021)

54. *Pandemia e gestione responsabile del conflitto. Le alternative alla giurisdizione. Atti del Convegno. Trento, 10 giugno 2021* - (a cura di) ANTONIO CASSATELLA, SILVANA DALLA BONTÀ, ELENA MATTEVI (2021)

55. *Il rapporto tra diritto, economia e altri saperi: la rivincita del diritto. Atti della* Lectio Magistralis *di Guido Calabresi in occasione della chiusura dell'anno accademico del Dottorato in Studi Giuridici Comparati ed Europei. Facoltà di Giurisprudenza. Trento, 24 ottobre 2019* - (a cura di) GIUSEPPE BELLANTUONO, UMBERTO IZZO (2022)

56. *Il contributo di Pietro Trimarchi all'analisi economica del diritto. Atti del Convegno. Trento, 16-18 dicembre 2020* - (a cura di) GIUSEPPE BELLANTUONO, UMBERTO IZZO (2022)

57. *Le relazioni fra Autonomie speciali e Regioni ordinarie in un contesto di centralismo asimmetrico: le complessità di una dialettica (1970-2020)* - (a cura di) ROBERTO TONIATTI (2022)

58. *Giustizia e mediazione. Dati e riflessioni a margine di un progetto pilota* - (a cura di) SILVANA DALLA BONTÀ, ELENA MATTEVI (2022)

59. ANTONIO ARMELLINI - *L'Italia e la carta di Parigi della CSCE per una nuova Europa. Storia di un negoziato (luglio-novembre 1990).* Introduzione di GIUSEPPE NESI. Postfazione di ETTORE GRECO. Con contributi di STEFANO BALDI, FABIO CRISTIANI, PIER BENEDETTO FRANCESE, NATALINO RONZITTI, PAOLO TRICHILO (2022)

60. *La rieducazione oggi. Dal dettato costituzionale alla realtà del sistema penale. Atti del Convegno. Trento, 21-22 gennaio 2022* - (a cura di) ANTONIA MENGHINI, ELENA MATTEVI (2022)

61. *La specialità nella specialità* - (a cura di) ROBERTO TONIATTI (2022)

62. *L'amministrazione condivisa* - (a cura di) GREGORIO ARENA, MARCO BOMBARDELLI (2022)

63. *Intelligenza artificiale e processo penale. Indagini, prove, giudizio* - (a cura di) GABRIELLA DI PAOLO, LUCA PRESSACCO (2022)

64. *L'attuazione della procura europea. I nuovi assetti dello spazio europeo di libertà, sicurezza e giustizia* - (a cura di) GABRIELLA DI PAOLO, LUCA PRESSACCO, ROSANNA BELFIORE, TOMMASO RAFARACI (2022)

65. *I rapporti tra attori pubblici e attori privati nella gestione dell'immigrazione e dell'asilo* - (a cura di) ELIANA AUGUSTI, SIMONE PENASA, STEFANO ZIRULIA (2022)

66. *Trasporto pubblico locale in fase pandemica e post-pandemica: alla ricerca del diritto alla mobilità in condizioni di sicurezza e di sostenibilità economica. Atti del Seminario. Trento, 5 aprile 2022* - (a cura di) ALESSIO CLARONI (2023) (pubblicazione disponibile solo on-line in Accesso Aperto: https://hdl.handle.net/11572/376915)

67. *Salute e carcere* - (a cura di) GABRIELE FORNASARI, ANTONIA MENGHINI (2023)

68. *La responsabilità da reato degli enti nel contesto delle cooperative agricole e vitivinicole. Atti del Convegno. Trento, 2 dicembre 2022* - (a cura di) ALESSANDRO MELCHIONDA, ENRICO PEZZI (2023)

69. *Percorsi interculturali* - (a cura di) CINZIA PICIOCCHI, DAVIDE STRAZZARI (2023) (pubblicazione disponibile solo on-line in Accesso Aperto: https://hdl.handle.net/11572/384871)

70. *Il diritto fra prospettiva rimediale e interpretazione funzionale. Atti delle* Lectiones Magistrales *di Salvatore Mazzamuto e Mario Barcellona in occasione della inaugurazione dell'anno accademico del Dottorato in Studi Giuridici Comparati ed Europei. Facoltà di Giurisprudenza. Trento, 6 aprile 2022* - (a cura di) UMBERTO IZZO (2023)

71. *Il principio di autoresponsabilità nella società e nel diritto*. *Atti del Convegno. Trento, 16 e 17 settembre 2022* - (a cura di) GABRIELE FORNASARI, TERESA PASQUINO, GIANNI SANTUCCI (2023)

72. *Giuristi d'impresa. La lettura del bilancio* - GIANLUCA CHIARIONI (2023)

73. *La riforma Cartabia tra non punibilità e nuove risposte sanzionatorie. Atti del Convegno. Trento, 24 e 25 marzo 2023* - (a cura di) ANTONIA MENGHINI, ELENA MATTEVI (2023)

74. *Il processo di riforma costituzionale cileno 2019-2023. Profili penalistici* - (a cura di) GABRIELE FORNASARI, CARLOS CABEZAS, EMANUELE CORN (2023)

75. *The Making of European Private Law: Changes and Challenges* - (ed. by) LUISA ANTONIOLLI, PAOLA IAMICELI (2024) (pubblicazione disponibile solo on-line in Accesso Aperto: https://hdl.handle.net/11572/401105)

76. *Il giudice di pace nel quadro delle riforme* - (a cura di) GABRIELE FORNASARI, ELENA MATTEVI, TERESA PASQUINO (2024) (pubblicazione disponibile solo on-line in Accesso Aperto: https://hdl.handle.net/11572/404351)

77. *COVID-19 Litigation. The Role of National and International Courts in Global Health Crises* - (ed. by) PAOLA IAMICELI, FABRIZIO CAFAGGI (2024) (pubblicazione disponibile solo on-line in Accesso Aperto: https://hdl.handle.net/11572/406169)

78. *Trasformazioni della giustizia. Norme, organizzazione, tecnologie* - (a cura di) GABRIELLA DI PAOLO (2024)

79. *Numérique & Environnement. Université d'été franco-italienne, Actes du colloque, 6-8 Juillet 2022, Université de Limoges* - (a cura di) LUISA ANTONIOLLI, MONICA CARDILLO, FULVIO CORTESE, LOUIS DE CARBONNIÈRES, FRANTZ MYNARD, CINZIA PICIOCCHI (2024) (pubblicazione disponibile solo on-line in Accesso Aperto: https://hdl.handle.net/11572/409990)

80. *Trento e la comparazione giuridica: voci, esperienze, riflessioni. Dalla testimonianza di Rodolfo Sacco e Mauro Cappelletti* - (a cura di) LUISA ANTONIOLLI, FULVIO CORTESE, ELENA IORIATTI, BARBARA MARCHETTI (2024)

81. *Il ruolo del Consiglio nella forma di governo delle autonomie speciali alpine: valorizzare e innovare* - (a cura di) MATTEO COSULICH, GIANFRANCO POSTAL, ROBERTO TONIATTI (2024)

82. *Beni a titolarità collettiva e sfruttamento della risorsa idrica. Il caso della Magnifica Comunità di Fiemme* - (a cura di) LUISA ANTONIOLLI, DAMIANO FLORENZANO, FLAVIO GUELLA, GIANFRANCO POSTAL (2024) (pubblicazione disponibile solo on-line in Accesso Aperto: https://hdl.handle.net/11572/412031)

83. *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future. Atti del convegno, Trento 29 settembre 2023* - (a cura di) ELISA CHIZZOLA, PAOLO GUARDA, VERONICA MARONI, LUIGI RUFO (2024)

84. *Studies on Argumentation & Legal Philosophy / 5. Una parola buona. Retorica e valori nella decisione giudiziale* - (Ed. by) MAURIZIO MANZIN, FEDERICO PUPPO, SERENA TOMASI (2024) (pubblicazione disponibile solo on-line in Accesso Aperto: https://hdl.handle.net/11572/421390)

85. *Prospettive di superamento del voto "tradizionale". Modelli di voto alternativi alla prova della compatibilità costituzionale* - (a cura di) ALESSANDRO DE NICOLA, VINCENZO DESANTIS (2024)

86. *Le transizioni e il diritto. Atti delle giornate di studio. 21-22 settembre 2023* - (a cura di) SIMONE FRANCA, ALESSANDRA PORCARI, SERGIO SULMICELLI (2024) (pubblicazione disponibile solo on-line in Accesso Aperto: https://hdl.handle.net/11572/434970)

87. *Lo studio dei papiri nei rivolgimenti metodologici della romanistica tra il 1860 e il 1960* - (a cura di) CHRISTIAN BALDUS, MASSIMO MIGLIETTA, TOMMASO BEGGIO, FILIPPO BONIN (2024)

88. *Il meccanismo unico di vigilanza: un bilancio dopo i primi dieci anni* - (a cura di) ANDREA MAGLIARI (2024)

89. *Stupefacenti e tossicodipendenza. Trattamento sanzionatorio, carcere e misure alternative* - (a cura di) GABRIELE FORNASARI, ANTONIA MENGHINI (2024)

90. *Mediare, riparare, conciliare. Giustizia riparativa e consensuale nel procedimento davanti al giudice di pace. Atti del Convegno. Trento, 3 maggio 2024* - (a cura di) SILVANA DALLA BONTÀ, GABRIELE FORNASARI, ELENA MATTEVI (2024) (pubblicazione disponibile solo on-line in Accesso Aperto: https://iris.unitn.it/handle/11572/441032)

91. *The teaching of Roman law in the 20th century: challenges and perspectives* - (a cura di) PAUL DU PLESSIS, TOMMASO BEGGIO (2024) (pubblicazione disponibile solo on-line in Accesso Aperto: https://hdl.handle.net/11572/441270)

92. *From multiculturalism to interculturalism: law, religious teaching and civic/citizenship education in today's Europe* - (ed. by) DAVIDE STRAZZARI with ROSSELLA BOTTONI, CINZIA PICIOCCHI (2025)

93. *Riparazione e giustizia riparativa nel sistema penale. Teorie, prassi e nuove prospettive. Atti del Convegno. Trento, 20 settembre 2024* - (a cura di) ANTONIA MENGHINI, ELENA MATTEVI (2025)

94. *Disabilità in movimento: percorsi di autodeterminazione* - (a cura di) LUCIA BUSATTA, PAOLO MACCHI, CARLA MARIA REALE (2025)

95. *Indagini e prove nella società digitale. Questioni attuali e prospettive future* - (a cura di) GABRIELLA DI PAOLO, LUCA PRESSACCO (2025)