SISTEMA PENALE

FASCICOLO

6/2023

ISSN 2704-8098

Sistema penale (*SP*) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.
La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.
La *Rivista* si uniforma agli standard internazionali definiti dal *Committe on Publication Ethics* (COPE) e fa proprie le relative linee guida.

Peer review I contributi che la direzione ritiene di destinare alla sezione "*Articoli*" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezione "*Altri contributi*" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.
Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen.* (o *SP*), 1/2022, p. 5 ss.

6/2023

PIATTAFORME CRIPTATE E PROVA PENALE

di Donatella Curtotti, Vittorio Rizzi, Wanda Nocerino, Annamaria Russitto, Giuseppe Giliberti, Gabriele Scarpa

*Ad oggi, le indagini penali sulle piattaforme criptate rappresentano una delle principali sfide che l'*environment law enforcement *si trova ad affrontare, ma da domani alle difficoltà di ordine tecnico – legate al fatto che si tratta di piattaforme dotate di importanti gradi di crittografia, con server spesso allocati in diversi Paesi del mondo – si affiancheranno criticità di natura giuridica in rapporto al corretto inquadramento delle attività espletate e alla conseguente diagnosi di utilizzabilità processuale dei dati raccolti. L'obiettivo dell'analisi è verificare la compatibilità delle investigazioni esperite sulle piattaforme criptate con le categorie probatorie già esistenti, al fine di accertare l'esistenza di una odierna copertura normativa idonea a garantire la tenuta costituzionale e codicistica degli elementi di prova acquisiti.*

SOMMARIO: 1. Le nuove frontiere dell'etere digitale. – 2. Criptofonini e *encrypted communication platforms*. – 3. Le inedite decisioni di legittimità. – 4. Quale statuto se… – 4.1. … le investigazioni sono condotte su *server* allocato in Italia. – 4.2. … le investigazioni sono condotte su *server* allocato in Paesi UE. – 4.3. Segue: … le investigazioni sono condotte su *server* allocato in Paesi *extra*-UE. – 5. Proposte.

1. Le nuove frontiere dell'etere digitale.

Si dice, ormai da tanto, che la rivoluzione informatica dell'ultimo tempo ha profondamente alterato le abitudini degli individui, incidendo sul modo di vivere, comunicare, interagire e intendere le relazioni interpersonali; di conseguenza, anche le modalità di concretizzazione delle più o meno tradizionali *species* delittuose sono mutate, plasmandosi in ragione di un rinnovato contesto sociale, politico ed economico.

Allo stesso tempo si sa che la metamorfosi culturale finisce per riflettersi sul sistema penale, condizionando le scelte di politica-criminale per adeguare la risposta statuale all'effettiva esigenza o emergenza da contenere[1]. Di qui, allo sviluppo tecnologico fa da *pendant* il mutamento ontologico delle fattispecie di reato: per un verso, la criminalità, abbattendo i troppo angusti confini interni, assume i connotati della

[1] Sottolinea il mutamento del sistema processuale sulla base dell'evoluzione sociale, già S. COTTA, *La sfida tecnologica*, Il Mulino, 1968, p. 179. Più di recente, G. SPANGHER, *Considerazioni sul processo "criminale" italiano*, Torino, 2015, p. 7 ss.

transnazionalità, dispiegando le sue potenzialità *ubicumque*; per l'altro, muta le sue caratteristiche tradizionali per manifestarsi interamente sulla Rete (c.d. *cybercrime*), ovvero per il tramite della Rete (c.d. *computer crime*)[2].

Sotto un profilo propriamente processuale, da anni si registra un frenetico ricorso a nuovi strumenti di indagine tecnologici che risultano indispensabili a rendere effettiva la lotta contro le più evolute forme di criminalità. Progredendo, infatti, con straordinaria velocità tanto le tecnologie di captazione - che diventano sofisticate ed invasive - quanto le modalità di elusione delle captazioni - che si affidano all'impenetrabilità degli apparecchi utilizzati, all'inaccessibilità di particolari reti di captazione ovvero all'adozione di sistemi di criptazione dei messaggi scambiati -, risulta imprescindibile ricorrere a nuovi strumenti investigativi ad alto potenziale tecnico per penetrare canali criminali di comunicazione o scambio di informazioni utilizzati per la commissione di reati di particolare allarme sociale.

A tali cambiamenti in chiave progressista, come detto, il giurista sembra oramai abituato: ha sperimentato l'uso del captatore informatico[3] e, poi, quello dell'*IMSI Catcher*[4]. Si pensava ingenuamente che il ritmo incalzante del progresso scientifico si fosse arrestato. E, invece, a distanza di pochi anni dalla tipizzazione normativa del *virus* informatico[5], la questione relativa all'impiego di nuove metodologie di indagine si impone con tutta la sua dirompenza.

L'ultima frontiera delle investigazioni è rappresentata dalle attività esperite sulle piattaforme di comunicazioni criptate, di recente utilizzate anche dalle organizzazioni criminali per condurre e pianificare i propri traffici illeciti. Questa volta non è lo strumento con cui l'investigazione viene esperita ad essere innovato ma la tecnica utilizzata per acquisire informazioni utili al processo: se in passato l'investigazione risultava circoscritta a specifici "ambienti" (come nel caso delle microspie) o a determinate aree di interesse (come nel caso del *virus Trojan)*, allo stato è l'etere digitale il nuovo spazio da "esplorare", cioè il *server* sul quale transitano tutti i flussi informativi degli utenti che utilizzano servizi di comunicazioni criptati[6]. Di conseguenza, cambiando lo spazio nel quale gli investigatori possono recuperare elementi di prova, cambiano anche le modalità con cui le indagini devono essere esperite.

---

[2] Per una trattazione approfondita delle tematiche esposte, cfr. AA. VV., Cybercrime. *Trattato di diritto penale,* a cura di A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA, Torino, 2019, p. 892 ss.

[3] Sul tema, volendo, W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Padova, 2021, *passim.*

[4] Per approfondimenti, A. CAMON, *Il cacciatore di IMSI*, in *Arch. pen.*, 2020, f. 1, p. 1 ss.; W. NOCERINO, *Il tramonto dei mezzi di ricerca della prova nell'era 2.0*, in *Dir. pen. proc.*, 2021, p. 1017 ss.

[5] Cfr. l. 23 giugno 2017, n. 103, d.lgs. 29 dicembre 2017, n. 216; d.l. 30 dicembre 2019, n. 161; l. 28 febbraio 2020.

[6] Sicuramente, già tramite l'uso del captatore informatico risulta ampliato a dismisura il raggio di azione dell'intercettazione, estesa alla folla indeterminata e indeterminabile di persone, anche estranee ai fatti di indagine, che in qualunque luogo conversano; tuttavia nel caso del *virus Trojan* è determinato il dispositivo oggetto di monitoraggio, mentre allorquando si compiono indagini su piattaforme criptate è il *server* (nella sua interezza) sul quale transitano le comunicazioni ad essere oggetto di indagine. Per una prima panoramica del tema in esame, M.T. MORCELLA, *La vicenda dei criptofonini in attesa della decisione della Cassazione,* in *Il penalista,* 6 aprile 2023.

Già da una prima analisi, emerge che quelle sulle *encrypted platforms* sono investigazioni assai complesse sia sotto il profilo operativo che giuridico. Da una parte, si tratta di indagare su piattaforme dotate di importanti gradi di crittografia con *server* spesso allocati in diverse parti del mondo, sfruttando le potenzialità offerte dai c.d. *big data*[7]; in questi casi, inevitabilmente, le forze di polizia necessitano della stretta collaborazione degli organi inquirenti di Stati diversi da quello in cui la necessità investigativa ha avuto origine[8]. Dall'altra, si profilano criticità di natura classificatoria, determinate dalla difficoltà di individuare la categoria probatoria in cui ascrivere le attività espletate su tali sistemi e, di conseguenza, emergono criticità relative alla diagnosi di utilizzabilità processuale dei dati ottenuti a seguito di decriptazione dei dati giacenti sui *server*.

Va, inoltre, precisato che in materia, il *law enforcement* nazionale è in netto ritardo rispetto agli altri Paesi europei, perché, ad oggi, l'Italia ha svolto un ruolo di "osservatore passivo" rispetto alle attività condotte da altri Paesi, posto che le forze di polizia italiane hanno ricevuto pacchetti di dati da analizzare ed eventualmente utilizzare secondo modalità definite da altri ma non hanno svolto alcuna attività investigativa autonoma sui *server* criptati che, peraltro, (almeno allo stato) non sono mai risultati allocati sul territorio nazionale.

Non è, però, inverosimile immaginare che di qui a qualche tempo le autorità nazionali si troveranno a ricoprire il ruolo di attori nelle investigazioni sulle piattaforme criptate.

Occorre interrogarsi sin d'ora circa la possibilità di svolgere "in prima persona" tali attività di indagine su *server* ubicati all'estero e/o in territorio nazionale.

In quest'ottica, il giurista è chiamato a comprendere se e in che termini le indagini sulle *encrypted communication platforms* possano trovare impiego nel processo penale, individuando la corretta cornice giuridica nella quale le attività possono essere sussunte.

---

[7] In argomento, AA. VV., *Big Data driven World: Legislation Issues and Control Technologies,* a cura di A.G. KRAVETS, Cham, 2019; AA. VV., *Trust, security and privacy for Big Data,* a cura di M. ALAZAB-M. GUPTA, Boca Raton, 2022; G.M. RUOTOLO, *I dati non personali: l'emersione dei* big data *nel diritto dell'Unione europea,* in *Studi sull'integrazione europea,* 2018, f. 1, p. 97 ss.

[8] Sul tema, *ex multis,* AA. VV., *Processo penale e regole europee: atti, diritti, soggetti e decisioni*, vol. II, a cura di F. RUGGIERI, Torino, 2018; AA. VV., *La nuova cooperazione giudiziaria penale. Dalle modifiche al Codice di procedura penale alla cooperazione giudiziaria penale*, a cura di M.R. MARCHETTI-E. SELVAGGI, coordinato da G. BARROCU, Milano, 2019; G. BARROCU, *Le speciali tecniche di investigazione nel contesto europeo,* in *Cass. pen.*, 2020, p. 1325 ss.; ID., *La cooperazione investigativa in ambito europeo. Da* Eurojust *all'ordine di indagine*, Padova, 2017; M. DANIELE, *Ricerca e formazione della prova*, in AA. VV., *Manuale di procedura penale europea*, a cura di R. KOSTORIS, Milano, 2022, V ed., Torino, p. 501 ss.; G. DE AMICIS, *Dalle rogatorie all'Ordine europeo di indagine: verso un nuovo diritto della cooperazione giudiziaria penale*, in *Cass. pen.*, 2018, f. 1, p. 22 ss.; L. MARAFIOTI, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento,* in AA. VV., *L'ordine europeo di indagine. Criticità e prospettive,* a cura di T. BENE-L. LUPARIA-L. MARAFIOTI, Torino, 2017; G. UBERTIS, *La prova acquisita all'estero e la sua utilizzabilità in Italia,* in *Cass. pen.*, 2014, p. 696 ss. Con precipuo riferimento alla circolazione transnazionale di prove digitali, D. CURTOTTI, *Indagini* hi-tech*, spazio* cyber*, scambi probatori tra Stati e* Internet provider service *e "Vecchia Europa": una normativa che non c'è (ancora)*, in *Dir. pen. proc.*, 2021, p. 745.

2. Criptofonini e *encrypted communication platforms*.

In tema di investigazioni tecnico-scientifiche, nessuna considerazione giuridica può prescindere dall'analisi del dato informatico, ossia dal confronto con le caratteristiche ontologiche dei prodotti della tecnologia quale prodromo essenziale per cogliere al meglio le riflessioni giuridiche che verranno svolte nel prosieguo; in questo senso, solo un preliminare vaglio circa il funzionamento dei criptofonini rende possibile l'individuazione delle problematiche che sottendono le indagini sulle piattaforme criptate e il conseguente impiego nel processo penale.

Un *cryptophone* – anche definito *Dedicated Encrypted Communication Devices* (DECD) – è un tipo di *smartphone* specificamente progettato per fornire comunicazioni sicure e proteggere da *hacking* e sorveglianza.

Si tratta, più precisamente, di dispositivi configurati come telefoni aziendali che presentano le medesime sembianze dei *devices* tradizionali ma che, nella sostanza, non si comportano come tali in quanto dotati di importanti sistemi di crittografia e cifratura che li rendono invulnerabili[9]: si tratta, dunque, di *smartphone* "modificati" a cui mancano molte delle funzionalità presenti in quelli in commercio[10].

Tutta la rete di comunicazione viene gestita attraverso un'infrastruttura realizzata dal fornitore dei servizi di criptofonia, con *server* sparsi in tutto il mondo, spesso collocati in Paesi "*offshore*". Inoltre, tali *devices* si servono delle *Hardened Secure Communication Platforms* (HSCP), più comunemente definite piattaforme di comunicazioni criptate, ossia di sistemi operativi e applicazioni installate su dispositivi

[9] Queste piattaforme non devono essere confuse con le più note applicazioni di messaggistica sicure, ovvero applicazioni di *chat* private che utilizzano algoritmi di cifratura (*end-to-end*) per proteggere i dati durante tutto il tragitto dal mittente al destinatario (quali, ad esempio, *Signal, Telegram, WhatsApp*). In questi casi, i dati vengono criptati al momento dell'invio e quindi decriptati una volta a destinazione. La differenza fondamentale delle applicazioni di messaggistica sicura con i criptofonini sta nel fatto che, in quest'ultimi, le comunicazioni in entrata e in uscita sono sempre crittografate *end-to-end* e vengono trasmesse su un canale crittografato per proteggere ulteriormente le informazioni. La configurazione di quest'ultimo *tunnel* avviene tramite una VPN (*Virtual Private Network*) dinamica e può essere modificata da remoto dagli amministratori.

[10] Nei criptofonini vengono disabilitati tutti quei servizi che possono essere facilmente intercettati, quali: la localizzazione GPS, i servizi *Google*, il *Bluetooth*, la fotocamera, i microfoni, la porta USB (che rimane in funzione solo per la carica della batteria). Anche l'uso di schede SD esterne viene interdetto. Rimangono attive le chiamate ma solo in modalità VoIP (*Voice over IP*), senza l'uso della rete GSM. Anche la messaggistica è presente ma utilizza applicazioni proprietarie e crittografate.

di comunicazione sicuri e protetti fisicamente. Le più note sono *EncroChat*[11] e *Sky ECC*[12], anche se in commercio ne esistono numerose e con differenti caratteristiche[13].

Le condizioni di vendita e di gestione dei criptofonini sono piuttosto proibitive[14], confermando la principale destinazione a supporto di attività illegali. Inoltre, nella maggior parte dei casi, vengono venduti per via "diretta", senza l'intermediazione di fornitori commerciali noti ma per il tramite di rivenditori sconosciuti (c.d. *reseller*).

Sotto il profilo strettamente tecnico, i criptofonini si servono di applicazioni e servizi dedicati che garantiscono l'inaccessibilità al sistema e la sicurezza dei dati *ivi* contenuti. Tra questi vanno ricordati:

a) *Zero-attack surface*. Tutti i punti di ingresso dei moderni dispositivi mobili – quali servizi Google, servizi GSM, SMS, *Bluetooth*, NFC, GPS, porta USB abilitata alla sola ricarica – vengono disabilitati.

b) *Trusted updates*. Gli aggiornamenti vengono emessi e firmati digitalmente esclusivamente attraverso il *Secure Administration System* (SAS): i dispositivi applicano gli aggiornamenti solo dopo aver verificato l'autenticità della firma digitale.

c) *Multiple password protection*. L'archiviazione, il sistema operativo e le applicazioni sicure del dispositivo sono tutti protetti da *passphrase* separate, ciascuna impostata per attivare una procedura di cancellazione in caso di errore per un numero consecutivo di volte.

d) *Multiple levels of encryption*. Le comunicazioni in entrata e in uscita sono crittografate *end-to-end* e trasmesse su una Rete crittografata (VPN). La configurazione

---

[11] *EncroChat* era una Rete di comunicazioni e un fornitore di servizi con sede in Europa che offriva *smartphone* modificati consentendo comunicazioni crittografate tra gli abbonati (circa 60 mila utenti). Si trattava di un *App* di messaggistica basata su OTR che instradava le conversazioni attraverso un *server* centrale con sede in Francia, *EncroTalk*, un servizio di chiamate vocali basato su ZRTP e *EncroNote*s, che consentiva agli utenti di scrivere note private crittografate. Il servizio di messaggistica crittografata *EncroChat* e i relativi telefoni personalizzati sono stati scoperti dalla gendarmeria francese nel 2017 che, poco dopo, ha provveduto a disattivare la piattaforma.

[12] *Sky Global* era una rete di comunicazioni e un fornitore di servizi con sede a Vancouver, in Canada: uno dei suoi prodotti più importanti era l'applicazione di messaggistica sicura *Sky ECC* e i criptotelefoni. nel 2021 erano oltre 171.000 gli apparati registrati, principalmente in Europa, Nord America, diversi Paesi del Centro e Sud America – principalmente Colombia – e Medio Oriente. Un quarto degli utenti attivi si trovava in Belgio (6.000) e nei Paesi Bassi (12.000). Una delle sue caratteristiche era l'autodistruzione dei messaggi dopo un periodo di scadenza definito dall'utente. Il sistema veniva utilizzato su telefoni appositamente modificati (Nokia, Google, Apple e BlackBerry) in cui la fotocamera, il microfono e il GPS venivano completamente disattivati; i messaggi venivano crittografati ed eliminati automaticamente dopo trenta secondi. Il 9 marzo 2021 Francia, Belgio ed Olanda, attraverso un'attività di indagine svolta a seguito della costituzione, sul canale giudiziario, di una squadra investigativa comune, sono riusciti a violare i *server* sui quali sono conservate le comunicazioni.

[13] Si pensi, solo per citarne alcuni, ad *Ennetcom, Exclu, Silent phone, Zphone, X1 e X1 black* della *Secure Group* e le piattaforme dall'azienda *Sikur*.

[14] Il prezzo per l'acquisto e la gestione di un criptofonino è alquanto elevato (fino a 1.500-2.000 € ogni sei mesi solo per avere l'abbonamento per il dispositivo) ed è dovuto principalmente alle SIM di *roaming* dati (SIM dedicate diverse da quelle dei *carrier* tradizionali che si collegano alla Rete di *server* messa a disposizione dal fornitore del servizio.).

VPN è dinamica e può essere modificata da remoto dagli amministratori. Anche tutti i dati memorizzati sul dispositivo sono crittografati.

e) *Encrypted VoIP*. Alcuni criptofonini consentono all'utente di camuffare la propria voce con una serie di *vocoder* digitali preconfigurati, tra cui: *robot* e generiche voci maschili e femminili.

f) *Volatile Data*. I dati possono essere distrutti: grazie a una cancellazione remota eseguita dal rivenditore per il tramite del *software Mobile Device Management* attivando una procedura tramite digitazione di un codice "antipanico" (c.d. *panic* o *SOS code*), per il cui tramite il dispositivo invia un messaggio automatico ai contatti di emergenza dell'utente. Ciò può avvenire dopo sette giorni (*default*) o anche meno dall'ultima accensione del dispositivo; dopo il riavvio del sistema (in alcune configurazioni); dopo un certo lasso di tempo in cui il dispositivo non è connesso alla Rete (ad esempio quando viene inserito in una borsa *faraday*); oppure qualora gli utenti immettano il proprio *passcode* quattro volte nella funzione di chiamata e poi compongono il numero.

g) *Data dissimulation*. Utilizzo di funzionalità anti-tracciamento, come IMEI, IMSI e *App* falsi per fuorviare i controlli di polizia.

h) *IMSI Catcher Detector*. Rileva ed evita la stazione base falsa nelle reti GSM/UMTS.

Sotto il profilo operativo, gli investigatori – non potendo interferire direttamente nella comunicazione poichè dotata di imponenti e pressochè invalicabili gradi di crittografia – hanno bisogno di "intromettersi" direttamente sul *server* per acquisire le informazioni utili alle indagini.

In questo contesto, si prospettano due possibilità investigative: procedere al *takedown*, ossia all'apprensione in blocco di tutti i dati giacenti sulla piattaforma attraverso il "congelamento" del *server*, oppure, penetrando la stessa, captare *live* il flusso di comunicazioni in transito.

3. Le inedite decisioni di legittimità.

La giurisprudenza, sul punto, si è già espressa. Come sempre accade quando si ha a che fare con strumenti di indagine inediti ad alto potenziale tecnologico, sono i giudici di legittimità – prima ancora del legislatore – ad intervenire per delineare i limiti e le condizioni di impiego dei risultati investigativi in sede processuale, molto spesso a seguito delle sollecitazioni provenienti dalle Corti sovranazionali e/o dalle Corti di altri Paesi[15].

[15] La similitudine non è casuale. Si pensi a quello che è accaduto nell'ordinamento nazionale allorquando ci si è imbattuto nelle investigazioni esperite per il tramite del captatore informatico. A ben guardare, infatti, prima ancora dell'intervento legislativo (cfr. nt. 5), è stata la giurisprudenza di legittimità a definire gli argini entro i quali concedere spazi di manovra al *virus* informatico (cfr. Cass., Sez. VI, 26 maggio 2015, n. 27100, in *Guida dir.*, 2015, f. 41, p. 83 s.; Cass., Sez. VI, 10 marzo 2016, n. 13884, in *Dir. inf. e informatica*, 2016, f. 1, p. 81; Cass., Sez. Un., 28 aprile 2016, n. 26889, in *Arch. pen.*, 2016, f. 2, p. 348 ss.), sollecitata dalla giurisprudenza europea. Infatti, quasi contemporaneamente alla sentenza delle Sezioni unite della Corte di cassazione italiana – pur nella diversità delle argomentazioni e conclusioni cui approda –, la Corte costituzionale

Non è un caso che, sulla scia di quanto sta accadendo in altri Stati europei[16], la questione relativa all'utilizzabilità dei dati acquisiti sui *criptophones* venga affrontata a più riprese dalla Suprema Corte con l'intento di delineare uno "statuto" delle investigazioni sulle piattaforme di comunicazione criptate[17].

Prima ancora di analizzare il contenuto delle pronunce che si susseguono freneticamente, occorre soffermarsi brevemente sul caso di specie da cui traggono origine le diverse decisioni in materia.

Pur non essendo ufficialmente noti i singoli passaggi investigativi che hanno portato all'apprensione degli elementi di prova mediante accesso ai *server* della società canadese (*Sky Global*) di *Sky ECC,* è dato sapere che l'indagine si è sviluppata – assumendo una dimensione internazionale – con l'istituzione di una squadra investigativa comune (*Joint Investigation Team*), composta dalle autorità giudiziarie e da rappresentanti delle forze di polizia di Belgio, Francia e Olanda, che ha operato con il supporto di *Eurojust* ed *Europol.*

Materialmente, l'acquisizione del contenuto della messaggistica avviene per il tramite delle autorità francesi – luogo in cui il *server* della società di *Sky ECC* è ubicato – secondo la previsione dell'art. 706-102-1 del *code de procédure pénale* che consente di accedere, conservare, registrare e trasmettere dati archiviati su sistemi informatici[18].

---

tedesca affronta il tema dei limiti alle investigazioni compiute con strumenti di sorveglianza occulta. Cfr. *Bundersverfassungsgericht*, 20 aprile 2016, 1 BVR 966/09, 1 BVR 1140/09.

[16] La Corte di cassazione francese, riprendendo la decisione del *Conseil Constitutionnel* dell'8 aprile 2022 sulla costituzionalità dell'art. 706-102-1 c.p.p. (*Conseil Constitutionnel*, 08 aprile 2022, QPC 2022-987, in *www.conseil-constitutionnel.fr*), riconosce l'applicabilità della disposizione al caso in esame, posto che gli inquirenti hanno legittimamente fatto accesso e acquisito i dati allocati sul *server*, secondo le prescrizioni del dettato normativo. In questo senso, Cass. Crim., 11 ottobre 2022, n. 21-85.148, in *www.legifrance.fr*, p. 1; Cass. Crim., 25 ottobre 2022, n. 21-85.763, *ivi*, p. 2. Cfr. anche le decisioni del Tribunale Superiore di Berlino e della Corte federale tedesca che sanciscono la piena utilizzabilità del materiale probatorio ottenuto mediante l'O.E.I. Cfr. *KG Berlin 2. Strafsenat*, 30 agosto 2021, 2 Ws 79/21, 2 Ws 93/21, in *www.gesetzeberlin.de*; *Bundesgerichtshof Beschluss*, 02 marzo 2022, 5 StR 457/21, in *www.juris.bundesgerichtshof.de.* Il medesimo risultato viene raggiunto anche in una recente decisione della Suprema Corte norvegese. Nella decisione HR-2022-1314-A, i giudici di legittimità ammettono l'acquisizione di dati informatici mediante la collaborazione tra forze di polizia. Cfr. *Supreme Court of Norway*, 30 giugno 2022, HR-2022-1314-A, in *www.domstol.no*.

[17] Si segnala che la giurisprudenza di legittimità si è pronunciata sul tema con diverse decisioni più o meno coeve. Cfr. Cass., Sez. IV, 5 aprile 2023, n. 16347, non massimata; Cass., Sez. VI, 25 ottobre 2022, n. 48330, in *C.E.D. Cass.*, n. 284027; Cass., Sez. I, 13 ottobre 2022, n. 6363, non massimata; Cass., Sez. IV, 15 luglio 2022, n. 32915, in *Giur. pen.*, con nota di A. BARBIERI, *I limiti di utilizzabilità dei messaggi crittografati scaricati da un server estero ed acquisiti mediante ordine europeo di indagine*; Cass., Sez. I, 1° luglio 2022, n. 34059, non massimata.

[18] La norma, modificata dall'art. 46, l. 23 marzo 2019, n°2019-222, sancisce che: «[P]uò essere necessario predisporre un dispositivo tecnico il cui scopo, senza il consenso degli interessati, è quello di accedere, ovunque, a dati informatici, di registrarli, archiviarli e trasmetterli, così come che siano archiviati in un sistema informatico, come vengono visualizzati su uno schermo per l'utente di un sistema automatizzato di elaborazione dati, poiché li introduce inserendo dei caratteri o mentre vengono ricevuti e trasmessi dalle periferiche. Il pubblico ministero o il giudice istruttore può nominare qualsiasi persona fisica o giuridica autorizzata ed iscritta in uno degli elenchi previsti dall'articolo 15T, al fine di compiere le operazioni tecniche che consentono la realizzazione del dispositivo tecnico di cui al primo comma del presente articolo. Il

L'operazione non rimane confinata ai Paesi direttamente interessati dall'operazione in parola: infatti, in diversi procedimenti penali nazionali, emerge la necessità di acquisire, mediante Ordine Europeo di Indagine (O.E.I.), la trascrizione dei messaggi scambiati da soggetti operanti su territorio italiano.

In un simile contesto, i giudici di legittimità – sollecitati dai difensori degli imputati talvolta per violazione delle norme in materia di intercettazione[19], talaltra per lesione del contraddittorio sulle modalità di apprensione delle *chat* allocate su *server* esteri[20] – sono stati chiamati a decidere sui limiti di impiego processuale dei "dati precostituiti", ovvero i contenuti della messaggistica scambiata per il tramite di criptofonini procacciati dalle forze di polizia di altri Stati europei e acquisiti per il tramite dell'O.E.I.

Più nel dettaglio, la Corte si trova ad affrontare la questione da un duplice angolo di visuale: da un lato, interviene per definire il corretto inquadramento giuridico delle attività di acquisizione del contenuto delle *chat* sulle piattaforme criptate e, dall'altro, per determinare le modalità attraverso cui i dati ottenuti all'estero possono transitare nel processo penale.

Con riferimento al primo aspetto, i giudici di legittimità[21] hanno sottolineato la necessità di distinguere due diverse tipologie di operazioni che gli inquirenti possono effettuare per acquisire informazioni su piattaforme di comunicazioni criptate. Precisamente, sotto il profilo tecnico, è possibile sia captare e registrare il messaggio cifrato nel mentre lo stesso è in transito dall'apparecchio del mittente a quello del destinatario, sia acquisire dati dopo aver provveduto a decriptare il contenuto delle conversazioni per trasformare mere stringhe informatiche in dati comunicativi intellegibili. A loro parere, nel primo caso si versa in un'ipotesi di intercettazione telematica, *ex* art. 266 *bis* c.p.p., posto che la captazione ha ad oggetto flussi comunicativi in transito; nel secondo, i messaggi archiviati sono sussumibili nell'alveo della prova documentale, acquisibile secondo le previsioni degli artt. 234 ss. c.p.p.[22].

Sulla base di tale ragionamento, i giudici hanno chiarito che, nel caso di specie, l'attività di acquisizione e di decifrazione dei dati comunicativi allocati su *server* esteri non possa rientrare nel novero delle intercettazioni, trattandosi invece di documenti informatici pienamente utilizzabili in conformità alle previsioni di cui all'art. 234 *bis* c.p.p.[23].

---

pubblico ministero o il giudice possono altresì prescrivere l'utilizzo di risorse statali soggette al segreto di difesa nazionale secondo le forme previste dal Capo 1 del Titolo IV del Libro 1».

[19] Cass., Sez. IV, 5 aprile 2023, n. 16347, cit.; Cass., Sez. I, 1° luglio 2022, n. 34059, cit.; Cass., Sez. I, 13 ottobre 2022, n. 6363, cit.

[20] Cass., Sez. VI, 25 ottobre 2022, n. 48330, cit.; Cass., Sez. I, 13 ottobre 2022, n. 6363, cit.; Cass., Sez. IV, 15 luglio 2022, n. 32915, cit.

[21] Cass., Sez. I, 1° luglio 2022, n. 34059, cit.; Cass., Sez. I, 13 ottobre 2022, n. 6363, cit.

[22] Cass., Sez. I, 1° luglio 2022, n. 34059, cit.

[23] Non è superflua la precisazione per cui i dati sono ubicati in uno Stato estero (ossia la Francia) e sono "di proprietà" dello Stato che presta il proprio consenso all'acquisizione degli stessi.

Con riferimento alle modalità acquisitive, per la Corte[24] i documenti informatici possono essere ottenuti e impiegati nel processo penale nazionale per il tramite dell'O.E.I., strumento di cooperazione investigativa cui ricorrere per favorire la circolazione delle prove nel Paesi *intra*-unionali[25].

In quest'ottica, secondo la giurisprudenza maggioritaria (in cinque pronunce su sette)[26], lo scrutinio sulla compatibilità del processo di acquisizione del dato probatorio con il diritto di difesa non risulta frustrato dalla scelta della procura di mettere a disposizione i soli esiti dell'attività svolta all'estero e non anche il percorso di acquisizione di quei dati[27], posto che l'autorità giudiziaria estera si è resa garante del rispetto delle corrette procedure acquisitive del dato informatico volte ad impedirne l'alterazione[28].

4. Quale statuto se...

Lo si è anticipato sin dalle prime battute del lavoro: il più complesso problema da risolvere è la tassonomia probatoria in cui ascrivere le attività di indagine esperite sulle piattaforme criptate. Questo perché i ritrovati della modernità non offrono solo nuove modalità di esecuzione di "vecchi" istituti processuali ma, spesso, rappresentano attività inedite, "casi" e "modi" originali che mal si conciliano con le categorie probatorie

[24] Cass., Sez. VI, 25 ottobre 2022, n. 48330, cit.; Cass., Sez. I, 13 ottobre 2022, n. 6363, cit.

[25] Sul punto, cfr. 4.2.

[26] Rilevante è la considerazione dei giudici di legittimità, per cui «[…] l'utilizzo di quella forma di cooperazione che, ai fini dell'acquisizione delle prove nell'ambito dell'Unione Europea, è rappresentata dall'O.E.I, è disciplinato dal d.lgs. 27 giugno 2017, n. 108, emanato per dare attuazione alla direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014. Nel sesto Considerando di tale direttiva si legge che nel programma di Stoccolma, adottato dal Consiglio europeo del 10-11 dicembre 2009, il Consiglio europeo ha considerato di perseguire ulteriormente l'istituzione di un sistema globale di acquisizione delle prove nelle fattispecie aventi dimensione transfrontaliera, basato sul principio del riconoscimento reciproco». Così Cass., Sez. I, 13 ottobre 2022, n. 6363, cit.

[27] Nello specifico la difesa lamenta che il p.m. ha messo a disposizione della difesa solo gli esiti dell'attività di polizia svolta, senza condividere il percorso (ovvero gli atti di indagine) che ha portato all'acquisizione delle *chat* decriptate e, in particolare, la documentazione di *Europol* (con i file decriptati) con l'indicazione precisa delle modalità di acquisizione dei dati nel *server* e gli annessi verbali di polizia. Cfr. Cass., Sez. VI, 25 ottobre 2022, n. 48330, cit.

[28] In una isolata pronuncia (Cass., Sez. IV, 15 luglio 2022, n. 32915, cit.), la Corte sostiene che l'acquisizione del dato probatorio (le *chat* decriptate) è inutilizzabile, poiché non è stato rispettato il diritto di difesa. Precisamente, la Cassazione afferma che il principio del contraddittorio implica una dialettica procedimentale non solo sugli esiti del materiale acquisito, ma anche sulle modalità con cui è stato acquisito detto materiale. Ne consegue che, *ex* art. 191 c.p.p., una prova è inutilizzabile se viola i divieti stabiliti dalla legge. In conclusione, per i giudici di legittimità, la difesa gode del diritto di accedere alla documentazione dell'attività investigativa svolta e di conoscere le modalità con cui erano state acquisite tali messaggi criptati, in virtù dell'osservanza del diritto di difesa e di contraddittorio.

esistenti e richiedono un'attenta analisi di tutti gli operatori del diritto sulla compatibilità con il sostrato giuridico in cui si insinuano[29].

Al fine di verificare la "legittimità probatoria" delle investigazioni sulle piattaforme criptate, prima ancora di affrontare le questioni inerenti alla qualificazione giuridica, occorre sgombrare il campo da un equivoco di fondo che potrebbe portare gli interpreti a negare *tout court* cittadinanza processuale ai dati acquisiti mediante le nuove tecniche di indagine.

Come noto, allo stato dell'arte, in Italia manca una previsione normativa che consente di accedere, acquisire e conservare dati informatici allocati presso *server* (interni o esteri), posto che l'attività rischia di trasformarsi in una sorveglianza massiva perpetua[30] ritenuta illegale perché in contrasto con le norme costituzionali (artt. 14 e 15 Cost.) e convenzionali (artt. 6 e 8 Cedu)[31].

A ben riflettere, però, le investigazioni sulle piattaforme criptate sono lontane dal rappresentare il prototipo delle tecniche di sorveglianza "non mirata" (o di massa), per cui «la persona, l'organizzazione o la caratteristica tecnica cui la raccolta dei dati è indirizzata non possono essere specificate preventivamente», rientrando, per converso, nell'ambito delle tecniche investigative di *surveillance* "mirata", ossia quelle «applicate dalle autorità competenti nel contesto di indagini penali [o prima del loro formale inizio] allo scopo di individuare e indagare su reati gravi e sospetti, e mirano a raccogliere

---

[29] Sull'assenza di una disciplina che indichi specificamente le modalità di acquisizione degli elementi di prova digitali, da ultimo, P. CORVI, *Le modalità di acquisizione dei dati informatici trasmessi mediante posta elettronica e applicativi di* chatting: *un* rebus *non ancora del tutto risolto,* in *Proc. pen. giust.,* 2023, f. 1, p. 216.

[30] La distinzione tra sorveglianza mirata e massiva viene ricavata dal *dictum* del Comitato di sorveglianza dei Servizi di *intelligence* e sicurezza (CTIVD), Relazione annuale 2013–2014, L'Aia, 31 marzo 2014, p. 45 s., per cui «si definisce sorveglianza di massa la raccolta da parte delle autorità di un'enorme quantità di informazioni su ciò che un gran numero di persone fa con il proprio telefono, *computer* o altri dispositivi "intelligenti" *on–line.* […] Questo è ciò che si intende per "sorveglianza" mirata, perché è rivolta ad una persona specifica che è sospettata di reati particolari. Questo tipo di interferenza con la *privacy* è compatibile con la normativa sui diritti umani solo se esistono garanzie a tutela dell'utilizzo di questi poteri di controllo da parte delle autorità e solo se viene esercitata nei confronti di reali autori di reato o terroristi. Si tratta infatti di un modo estremamente efficace per raccogliere prove, anche se per monitorare continuamente un sospettato sono necessari molto personale e molto denaro. A differenza della sorveglianza mirata, la sorveglianza di massa non è incentrata su singoli individui. […] La sorveglianza di massa è talvolta definita come una sorveglianza "non targetizzata" o "in rete". Si riferisce ad una situazione in cui centinaia di migliaia o milioni di informazioni vengono raccolte ogni giorno in un determinato paese su centinaia di migliaia o milioni di persone». Sul punto, più di recente, A.G. FERGUSON, *Persisten surveillance,* in *Alabama Lae Review,* 2022, p. 3; E. BALKOVICH-D. PROSNITZ-A. BOUSTEAD-S.C. ISLEY, *Electronic Surveillance of Mobile Devices. Understanding the Mobile Ecosystem and Applicable Surveillance Law,* Rand Coroporation, 2022, p. 13 ss.

[31] Come precisa la Corte EDU, sussiste una violazione dell'art. 6, comma 2, Cedu tutte le volte in cui l'autorità giudiziaria non ha indicato in maniera esaustiva i motivi che hanno determinato la compressione delle libertà fondamentali. Corte EDU, 26 giugno 2016, *Mugosa c. Montenegro*; Corte EDU, 10 novembre 2015, *Slavov e altri c. Bulgaria*. Inoltre, sussiste una violazione dell'art. 8 Cedu ogniqualvolta il provvedimento con cui vengono disposte le intercettazioni non viene corredato da una solida motivazione quanto ai suoi presupposti; nondimeno, è compito dell'autorità monitorare con costanza la permanenza delle ragioni che, ai tempi, imponevano la captazione occulta. Da ultimo, Corte EDU, 12 gennaio 2023, *Potoczka and Adamco c. Slovacchia.*

informazioni in modo tale da non avvisare le persone bersaglio»[32]. In questi casi, infatti, pur se l'investigazione non è diretta ad acquisire flussi comunicativi di sistemi informatici "determinati" ma tutti i flussi che transitano (o sono transitati) sulla piattaforma, esiste un *target* di riferimento, così come esiste ed è sufficientemente individuato un "sistema" da attenzionare, sia pur virtuale ed etereo, quale è il *server*.

Dunque, posto che le indagini sulle piattaforme criptate non rientrano nel *genus* della sorveglianza di massa, l'interprete è tenuto a compiere uno sforzo ermeneutico ulteriore, al fine di comprendere se e in che termini le nuove tecniche investigative possano trovare riscontro negli istituti processuali più o meno noti al sistema. La legittimità degli atti di indagine provenienti dalle investigazioni sulle *encrypted communication platforms* è, infatti, strettamente connessa alla qualifica giuridica ad essi riconosciuta: solo qualora tali atti dovessero rientrare nell'ambito delle categorie probatorie già sperimentate dal sistema non sarebbe preclusa la possibilità di utilizzare gli atti di indagine nel processo.

Di qui, posta la centralità del tema nel dibattito futuribile, nel prosieguo della trattazione si verificherà la compatibilità delle attività esperite sulle piattaforme criptate con gli istituti tipizzati dal legislatore, proponendone l'artificiosa partizione sulla base della tipologia di attività esperita dagli inquirenti, in modo tale da ricondurre ciascuna operazione sotto l'egida del mezzo probatorio più affine, al fine di accertare l'esistenza di una copertura normativa.

Un dato, però, va immediatamente sottolineato: i profili differenziali della tecnica investigativa rispetto alle categorie probatorie "tradizionali" rendono complessa l'opera di sussunzione delle attività esperite sulle piattaforme criptate nell'alveo dei mezzi di ricerca della prova già noti al sistema. Eppure, non potendo arrendersi all'idea che le nuove indagini finiscano per rimanere improficue a causa di una normativa obsoleta, l'interprete deve compiere uno sforzo ermeneutico per adeguare, nel rispetto dei principi dell'ordinamento giuridico, la disciplina vigente alle nuove sfide dell'era moderna.

Al di là delle difficoltà evidenziate, si riscontrano ulteriori criticità in rapporto al "luogo" in cui è allocato il *server*, posto che, qualora questo fosse ubicato oltre i confini del territorio nazionale, entrerebbero in gioco gli strumenti di cooperazione investigativa che, come meglio si dirà nel prosieguo, non sempre sono idonei a garantire la raccolta transnazionale dei dati informatici. Perciò, si tenterà di discernere tre scenari possibili di intervento che differiscono a seconda del luogo in cui è ubicato il *server* su cui confluiscono i dati da apprendere, distinguendo, per ciascuna ipotesi, le attività esperibili a seconda che siano condotte dall'Italia come "osservatore passivo" – ossia quando vengono richiesti gli esiti delle indagini esperite da altri Paesi, ovvero dati precostituiti – oppure che si tratti di investigazioni "*live*" condotte dallo Stato nazionale.

[32] Sul punto, Assemblea Generale, A/69/397, 23 settembre 2014, cfr. *www.europarl.europa.eu*.

4.1. … le investigazioni sono condotte su server allocato in Italia.

La prima ipotesi da vagliare inerisce al caso in cui il *server* sul quale transitano le comunicazioni criptate sia allocato sul territorio nazionale.

In questo contesto, al fine di individuare la corretta veste giuridica da attribuire alle attività investigative compiute in Italia, occorre distinguere a seconda che l'acquisizione di comunicazioni avvenga contestualmente alla trasmissione dell'informazione ovvero in un momento successivo allo scambio comunicativo.

Circoscrivendo l'analisi all'ipotesi in cui l'azione acquisitiva sia "*live*" – e, dunque, la captazione avvenga nel momento in cui la comunicazione transita nell'etere digitale –, la categoria probatoria con cui sembra opportuno confrontarsi è rappresentata dalle intercettazioni telematiche, regolate dall'art. 266 *bis* c.p.p.[33], che, come noto, hanno ad oggetto un «flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi»[34], ossia tra *computer* collegati tra loro in Rete, via modem, via radio (se i dispositivi sono connessi con tecnologia *wireless*) o con qualsiasi altra forma di interconnessione.

Tale flusso può essere rappresentato non solo dal tradizionale scambio di *e-mail* o per mezzo delle più svariate applicazioni che consentono l'interazione in tempo reale o differito (servizi di messaggistica e di *chat*) ma anche da *file* sonori e comunicazioni vocali che, come statuito dalla giurisprudenza di legittimità, «rappresentano a tutti gli effetti un flusso di dati»[35].

Sicuramente, sotto il profilo tecnico-operativo, l'accesso ad un *server* per captare comunicazioni in atto può essere ricompreso nell'alveo delle intercettazioni telematiche, venendo in rilievo il carattere della contestualità della captazione di un flusso comunicativo tra sistemi collegati in Rete.

Tuttavia, pur volendo assimilare tali forme captative alle intercettazioni "classiche", non si può negare che le prime siano caratterizzate da significative peculiarità, risultando molto più intrusive per chi vi è sottoposto e, al contempo, assai più efficaci per i loro esiti istruttori.

Si converrà che un conto è captare flussi telematici intercorrenti tra due o più sistemi oggetto di intercettazione, ben altro è accedere direttamente al *server* sul quale

---

[33] Per tutti, M. TORRE, *L'intercettazione di flussi telematici (art. 266* bis *c.p.p.)*, in AA. VV., Cybercrime, cit., p. 1472 ss.

[34] Il "flusso" può essere definito come il susseguirsi di comunicazioni in corso all'interno di un sistema o tra più sistemi informatici, tra i quali è possibile uno scambio di impulsi che trasmettono informazioni. Per "sistema informatico" deve intendersi qualunque complesso di apparecchiature destinate a compiere qualsiasi funzione utile all'uomo attraverso l'impiego di tecnologie informatiche. Le comunicazioni tra sistemi informatici – che si concretano in segnali digitali (dati binari o *bit*) avvengono lungo linee non telefoniche, come quelle impiegate per mettere in collegamento, con l'ausilio di apposite apparecchiature (*server*), varie postazioni informatiche (*Local Area Network*). In un sistema telematico, invece, la trasmissione dei dati avviene lungo la linea telefonica, televisiva o satellitare. Una simile differenziazione è fatta propria dalla giurisprudenza di legittimità. Da ultimo, Cass., Sez. V, 8 gennaio 2020, n. 4470, in *C.E.D. Cass.*, n. 277855.

[35] Così Cass., Sez. Un., 13 luglio 1998, n. 21, in *Cass. pen.*, 1992, f. 2, p. 465.

transitano tutte le comunicazioni di tutti gli utenti che utilizzano quel servizio. Di qui, si potrebbe dubitare del fatto che tali attività possano essere sussunte nella disciplina di cui all'art. 266 *bis* c.p.p., che, come precisato, «consente limitazioni mirate»[36], circoscrivendo l'ambito della captazione nel pieno rispetto dei *dicta* costituzionali e convenzionali[37].

Se questa è un'eccezione condivisibile, sembra possibile un'interpretazione "evolutiva" del dettato normativo, peraltro suggerita dalla giurisprudenza della Corte EDU, per cui «deve ritenersi sufficiente che il decreto autorizzativo indichi il destinatario della captazione e la tipologia di ambienti ove questa viene condotta»[38]. E, allora, così ragionando, il *server* potrebbe essere considerato come un contenitore (*rectius:* spazio) su cui transitano flussi comunicativi da attenzionare, non dissimile dallo *smartphone* o dal *computer*.

Si potrebbe, in altri termini, arrivare ad affermare che tale captazione rappresenti un'evoluzione dell'intercettazione telematica "tradizionale" avendo ad oggetto flussi comunicativi transitanti su un nuovo "sistema informatico", ossia il *server*, posto che è proprio quello spazio a dover essere "monitorato" perché è sul nuovo ambiente virtuale che (presumibilmente) si consuma il fatto di reato.

L'approccio è parzialmente difforme nel caso in cui gli investigatori decidano di non procedere a captazioni "*live*" di un flusso comunicativo in transito su sistemi informatici ma acquisiscano dati precostituiti direttamente "alla fonte", attraverso l'apprensione del *server* in quanto corpo del reato.

In tale ipotesi, si profilano dubbi e perplessità circa il corretto inquadramento delle attività *de quibus*, perennemente in bilico tra differenti istituti processuali, quali le intercettazioni di flussi telematici (art. 266 *bis* c.p.p.), il sequestro di corrispondenza (art. 254 c.p.p.) e il sequestro probatorio di dati informatici (art. 253 c.p.p.).

Tradizionalmente, come chiarito dalla giurisprudenza di legittimità[39], i messaggi conservati nella memoria di un cellulare devono essere considerati documenti, ai sensi dell'art. 234 c.p.p., posto che gli stessi «non rientrano nel concetto di "corrispondenza", in quanto quest'ultima implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito […]»; e nemmeno può ritenersi che si

---

[36] Così L. FILIPPI, sub *art. 266* bis, in AA. VV., *Codice di procedura penale commentato,* a cura di A. GIARDA-G. SPANGHER, Milano-Padova, 2023.

[37] Sul punto la dottrina è assai vasta. *Ex plurimis*, A. BALSAMO, *Intercettazioni: gli* standards *europei, la realtà italiana e le prospettive di riforma,* in *Cass. pen.*, 2009, f. 10, p. 4023 ss.; A. DIDDI, *L'inviolabilità della segretezza delle comunicazioni*, in AA. VV., *Processo penale e costituzione*, a cura di F.R. DINACCI, Milano, 2010, p. 274 ss.; S. FURFARO, *Un problema irrisolto: le intercettazioni telefoniche*, in AA. VV., *Procedura penale e garanzie europee,* a cura di A. GAITO, Torino, 2006, p. 117; A. GAITO-S. FURFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza,* in AA. VV., *I principi europei del processo penale*, a cura di A. GAITO, 2016, p. 363 ss.; G. UBERTIS, *Principi di procedura penale europea. Le regole sul giusto processo*, Milano, 2000, p. 105 ss. Con precipuo riferimento al tema delle intercettazioni, per tutti, A. BARGI, *L'elusione delle garanzie sostanziali convenzionali nella riforma delle intercettazioni tra illusione (la tutela della privacy) e realtà,* in AA. VV., *Regole europee e processo penale*, a cura di A. GAITO-D. CHINNICI, 2018, Milano-Padova, 2018, p. 87 ss.

[38] Sul punto Corte EDU, 4 dicembre 2015, *Roman Zakharov c. Russia*.

[39] Cass., Sez. VI, 6 febbraio 2020, n. 12975, in *C.E.D. Cass.*, 278808; Cass., Sez. VI, 28 maggio 2019, n. 28269, *ivi,* n. 276227.

tratti degli esiti di un'attività di intercettazione «la quale postula, per sua natura, la captazione di un flusso di comunicazioni in atto. […] i dati presenti sulla memoria del telefono acquisiti *ex post* costituiscono mera documentazione di detti flussi»[40].

Di conseguenza – secondo la Corte[41] – l'acquisizione di tali testi non può essere sottoposta né alle regole applicate per il sequestro di corrispondenza (art. 254 c.p.p.), nè alle previsioni in materia di intercettazioni telematiche (artt. 266 *bis* c.p.p.), ma alla disciplina di cui all'art. 253 c.p.p., trattandosi di documenti informatici dal contenuto comunicativo[42].

Seguendo un simile ragionamento, allorquando vengono acquisiti messaggi conservati sul *server*, la relativa attività non può soggiacere alla disciplina stabilita per la corrispondenza: nel caso di specie, infatti, si procede a "congelare" il *server* quale contenitore di informazioni per acquisire *ex post* un dato conservato in un *macro* contenitore che documenta flussi di comunicazioni già avvenuti. Di qui, almeno sotto il profilo tecnico-operativo, la relativa attività potrebbe essere ricompresa nell'ambito del sequestro probatorio di dati informatici, secondo le previsioni di cui all'art. 253 c.p.p.

Deve, tuttavia, evidenziarsi che anche tale procedura sussuntiva non è scevra da criticità. Come noto, infatti, il decreto di sequestro probatorio, anche ove abbia ad oggetto cose costituenti corpo di reato, deve contenere una specifica motivazione sulla finalità perseguita per l'accertamento dei fatti[43] e deve essere finalizzato all'apprensione solo di quanto sia effettivamente utile ai fini di indagine[44], nel pieno rispetto del principio di proporzionalità[45]. In giurisprudenza, infatti, si afferma che l'estrazione di copia integrale dei dati, contenuti in dispositivi informatici o telematici sottoposti a sequestro probatorio, realizza solo una copia-mezzo che consente la restituzione del dispositivo

---

[40] Così Cass., Sez. I, 2 dicembre 2020, n. 461, in *questa Rivista*, 29 marzo 2021; Cass., Sez. VI, 12 dicembre 2019, n. 1822, in *C.E.D. Cass*., n. 278124. Delineano l'acquisizione della messaggistica istantanea quale sequestro di documenti informatici, Cass., Sez. V, 21 novembre 2017, n. 1822, in *Giur. it.*, 2018, f. 7, p. 1817 ss. Da ultimo, Cass., Sez. V, 7 ottobre 2021, n. 3591, in *Cass. pen.* 2022, p. 3106, con nota di A. PROCACCINO, *Piccoli equivoci senza importanza: tra intercettazioni di flussi informatici, perquisizioni e prove atipiche.* In dottrina, per tutti, F. ZACCHÈ, *L'acquisizione della posta elettronica nel processo penale,* in *Proc. pen. giust.*, 2013, f. 4, p. 103 ss.

[41] Cass., Sez. VI, 28 maggio 2019, n. 28269, cit.

[42] Più in generale, il documento informatico, *species* della prova digitale, è un documento non cartaceo formato dai programmi (*software*) di un calcolatore elettronico e, contemporaneamente, alla sua formazione, registrati in un apposito spazio dal calcolatore medesimo (*hardware*) o su strumenti di supporto elettronico o digitale. Si potrebbe, dunque, definire il documento informatico come «un qualsiasi *file* avente un elemento rappresentativo espresso in un linguaggio binario». Così G. VACIAGO, *Profili processuali delle indagini informatici*, in AA. VV., *Diritto dell'internet*, a cura di G. CASSANO-G. SCORZA-G. VACIAGO, Padova, 2013, p. 640. Può trattarsi, quindi, di un testo, di un'immagine, di un suono, o anche di una pagina *web* o di una *e-mail*. Sul tema, per tutti, P. TONINI, *L'evoluzione delle categorie tradizionali: il documento informatico,* in AA. VV., Cybercrime, cit., p. 1308 ss.; ID., *Documento informatico e giusto processo,* in *Dir. pen. proc.*, 2009, p. 401.

[43] Cfr. Cass. Sez. Un., 19 aprile 2018, n. 36072, in *Proc. pen. giust.*, 2019, con nota di M.F. CORTESI, *Sequestro del corpo del reato e onere motivazionale: dopo un tormentato dibattito interpretativo raggiunto "forse" un punto fermo*.

[44] In questo senso, M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale,* in *Dir. pen. cont.*, 18 giugno 2014.

[45] Sul punto, più di recente, L. ALGERI, *Principio di proporzionalità e sequestro probatorio di sistemi informatici,* in *Dir. pen. proc.*, 2020, p. 850; G. CASCONE, *Il sequestro informatico nel prisma del principio di proporzione, ivi,* 2022, p. 123.

ma non legittima il trattenimento della totalità delle informazioni apprese oltre il tempo necessario a selezionare quelle pertinenti al reato per cui si procede[46].

Va, tuttavia, evidenziato che anche questa "regola" di matrice giurisprudenziale non è immune da eccezioni: in alcune pronunce, infatti, la Corte di legittimità esclude la violazione del principio di proporzionalità laddove il sequestro dell'intero contenuto di un sistema informatico sia necessitato da specifiche esigenze probatorie che vengono in rilievo sulla base delle peculiarità del fatto di reato per il quale si procede[47].

Di conseguenza, non sussisterebbero ragioni ostative all'acquisizione di un *server* (e del suo contenuto) allorquando il decreto che dispone la misura contenga la precisa indicazione delle ragioni che giustificano l'estensione dell'apprensione, in modo tale da consentire un controllo postumo sulla proporzionalità del vincolo apposto sui dati informatici.

4.2. … le investigazioni sono condotte su server *allocato in Paesi UE.*

La seconda ipotesi da considerare inerisce al caso in cui il *server* da monitorare sia ubicato in uno Stato membro dell'Unione europea; ipotesi, invero, assai più nota nella prassi giudiziaria e affrontata a più riprese dalle Corti nazionali[48].

L'indiscusso punto di riferimento delle investigazioni unionali è rappresentato dall'O.E.I. che, oramai da qualche tempo, travolge le forme di cooperazione tradizionali allorquando l'indagine è relegata nei confini dell'Unione Europea[49].

L'ambito di applicazione dell'istituto può comprendere, sia nella fase "passiva" che "attiva", tutti gli atti di indagine e di ricerca della prova espressamente indicati dalla

---

[46] Cass., Sez. VI, 22 settembre 2020, n. 34265, in *Cass. pen.*, 2021, p. 1001. Nello stesso senso, Cass., Sez. VI, 4 marzo 2020, n. 13156, in *C.E.D. Cass.*, n. 279143.

[47] In questo senso, Cass., Sez. Un., 20 luglio 2017, n. 40963, in *Cass. pen.*, 2018, p. 131.

[48] Si tratta del caso affrontato dalla giurisprudenza di legittimità. Cfr. § 3.

[49] Come è stato acutamente osservato, la direttiva in parola non rappresenta una vera e propria rivoluzione. In questo senso M. CAIANIELLO, *L'OEI dalla direttiva al decreto n. 108 del 2017*, in AA. VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017*, a cura di M. DANIELE-R.E. KOSTORIS, Torino, 2018, p. 2, per cui «il sistema dell'O.E.I. risulta influenzato, tanto nella direttiva quanto nel decreto legislativo di recepimento, da due modelli culturali differenti, che tra loro si intersecano per dar vita ad una forma ibrida». Secondo A. CABIALE, *I limiti alla prova nella procedura penale europea*, Milano-Padova, 2019, p. 250, «tale disciplina costituisce […] una mera opera di unificazione volta ad assorbire le Convenzioni di assistenza giudiziaria del 1959 e del 2000, nonché quella di applicazione dell'accordo di Schengen, oltre alle decisioni quadro 2003/577/GAI sull'esecuzione dei provvedimenti di blocco dei beni o di sequestro e 2008/879/GAI in tema di mandato europeo di ricerca delle prove». Nello stesso senso, M. CAIANIELLO, *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione delle prove,* in *Proc. pen. giust*., 2015, f. 3, p. 1; M. DANIELE, *L'ordine europeo di indagine entra a regime. Prime riflessioni sul d.lgs. 108 del 2017*, in *Dir. pen. cont*., 28 luglio 2017; E. LORENZETTO, *L'ordine europeo di indagine penale: efficienza e garanzie per le acquisizioni probatorie in àmbito eurounitario,* in *Cass. pen*., 2020, f. 3, p. 1302 ss.; A. MANGIARACINA, *L'acquisizione "europea" della prova cambia volto: l'Italia attua la direttiva relativa all'ordine europeo di indagine penale*, in *Dir. pen. proc*., 2018, p. 158 ss.; F. RUGGIERI, *Le nuove frontiere dell'assistenza penale internazionale: l'ordine europeo di indagine penale*, in *Proc. pen. giust.*, 2018, f. 1, p. 12 ss.; A. SCALFATI, *Note minime su cooperazione investigativa e mutuo riconoscimento,* in *ivi*, 2017, f. 2, p. 217 ss.

direttiva 2014/41/UE: sicuramente di precipuo interesse, quanto alle indagini relative al *cybercrime*, sono le richieste di dati del traffico telefonico e/o di intercettazioni di comunicazioni e le operazioni sotto copertura.

Per quanto attiene alle attività investigative tipiche volte alla captazione di conversazioni e comunicazioni, con l'istituzione dell'O.E.I. viene regolamentata la procedura esecutiva delle intercettazioni transfrontaliere, anche se effettuate per via telematica, da esperire allorquando il dispositivo (o il sistema) da controllare si trovi in uno Stato membro[50].

In effetti, sia la direttiva 2014/41/UE[51] che il d.lgs. 108/2017[52] dedicano particolare attenzione all'istituto in esame, riferendosi, in modo particolare, alle «intercettazioni di telecomunicazioni»[53], qui da intendersi come captazioni di conversazioni o flussi comunicativi che si avvalgono dell'ausilio di strumenti tecnici, quali il telefono o il *computer*.

In questo senso, ricorrendo ad un'interpretazione estensiva del dettato normativo[54], anche la captazione di flussi comunicativi in transito su *server* allocati all'estero può essere sussunta nell'ambito delle intercettazioni di telecomunicazioni e, dunque, può essere esperita mediante ricorso all'O.E.I.

Qualora, però, l'operazione investigativa non è deputata alla richiesta di esperimento di intercettazioni telematiche all'estero ma è finalizzata all'acquisizione di informazioni "precostituite", ossia elementi di prova che rappresentano il frutto di attività investigative condotte in altri Paesi, la procedura è parzialmente difforme.

---

[50] Con riferimento alle intercettazioni transfrontaliere, il Considerando n. 31 della direttiva 2014/41/UE, stabilisce che «[S]e più Stati membri sono in grado di fornire l'assistenza tecnica necessaria, l'O.E.I. dovrebbe essere trasmesso solo a uno di essi e la priorità dovrebbe essere attribuita allo Stato membro in cui si trova la persona interessata. Gli Stati membri in cui si trova la persona sottoposta a intercettazione, e la cui assistenza tecnica non è necessaria per effettuare l'intercettazione, dovrebbero riceverne notifica conformemente alla presente direttiva. Tuttavia, sebbene l'assistenza tecnica non possa essere ricevuta da un solo Stato membro, l'O.E.I. può essere trasmesso a più Stati di esecuzione».

[51] La direttiva affronta il tema delle intercettazioni sia nei Considerando nn. 30-31, che, soprattutto nel Capo V, negli artt. 30 e 31, rubricato "*Intercettazioni di telecomunicazioni*".

[52] Più precisamente, agli artt. 23-25 sono dedica le regole inerenti alla procedura passiva, mentre agli artt. 43-45, quelle per la procedura attiva.

[53] Coma premesso, nel Considerando n. 30 della direttiva 2014/41/UE si legge che «[L]e possibilità di cooperare conformemente alla presente direttiva in materia di intercettazione delle telecomunicazioni non dovrebbero essere limitate al contenuto delle telecomunicazioni, ma dovrebbero anche riguardare la raccolta di dati relativi al traffico e all'ubicazione associate a tali telecomunicazioni, in modo che le autorità competenti possano emettere un O.E.I. inteso a ottenere dati meno intrusivi sulle telecomunicazioni […]». Anche se, come acutamente rilevato, la previsione del Considerando in parola non è riproposta nell'articolato testo normativo, per cui si potrebbe ritenere che tali operazioni non possono essere già autonomamente disposte od eseguite, dovendo essere "associate" alle intercettazioni vere e proprie. In questo senso, C. MARINELLI, *Le intercettazioni di comunicazioni*, in AA. VV., *L'ordine europeo di indagine penale*, cit., p. 232 s. *Contra* F. NANNI, *Le intercettazioni telefoniche*, in AA. VV., *La nuova cooperazione giudiziaria penale*, cit., p. 484 ss., per cui, «[N]essun dubbio, invece, [sussiste] in rapporto alla regolamentazione dell'acquisizione transfrontaliera dei c.d. dati esterni delle comunicazioni».

[54] Sulle considerazioni relative alla sussunzione dell'attività in esame nell'ambito delle intercettazioni telematiche, cfr. § 4.1.

Seguendo il ragionamento già condotto con riferimento alle acquisizioni su *server* allocato in territorio italiano[55], l'attività di captazione di messaggi archiviati su piattaforme criptate non può essere assoggettata alla disciplina delle intercettazioni (venendo meno la contestualità della comunicazione), trattandosi di documenti aventi contenuto comunicativo. In quest'ottica, l'O.E.I. risulta funzionale a raccogliere i risultati di atti di indagine già esperiti nel territorio dello Stato estero, secondo la previsione del dettato di cui all'art. 234 *bis* c.p.p.[56].

Tradizionalmente, come anche chiarito dalla giurisprudenza, «l'attività di intercettazione di dati tra dispositivi che usano il sistema criptato *pin to pin*, seguendo la tecnica dell'instradamento, non richiede l'espletamento di formule rogatoriali sempre che (perlomeno) uno dei conversanti si trovi sul territorio italiano; la trasposizione in comunicazioni intellegibili, intervenuta tramite il consenso del gestore estero del *server* informatico sul quale sono depositati i relativi dati, non richiede la procedura contemplata dagli artt. 266 ss., potendo l'autorità giudiziaria ricorrere all'acquisizione documentale contemplata dall'art. 234 *bis* c.p.p.»[57].

Nonostante gli ultimi approdi giurisprudenziali, deve ammettersi che il ricorso all'O.E.I. potrebbe profilare alcune criticità in rapporto al principio di legalità della prova, al quale il sistema della cooperazione transfrontaliera è informato: infatti, sia l'art. 1, § 4 della direttiva 2014/41/UE che l'art. 1, d.lgs. 108/2017 sanciscono il dovere di rispettare i principi dell'ordinamento costituzionale e della Carta dei diritti fondamentali dell'Unione Europea[58]. Inoltre, pur rimettendo alle scelte dei singoli Stati la valutazione probatoria degli elementi investigativi raccolti all'estero[59], nell'articolato legislativo sono previste – più o meno esplicitamente – regole di esclusione delle prove acquisite *contra legem*. Solo a titolo esplicativo, si pensi all'art. 6, § 1 della direttiva, trasposto nell'art. 27 del decreto in rapporto all'inutilizzabilità delle prove acquisite in violazione dei requisiti nazionali di ammissibilità, all'art. 9, § 2 della direttiva, trasfuso nell'art. 4, commi 2, 3 e 5 del decreto in rapporto alle prove acquisite violando le norme sul *quomodo* delle attività istruttorie, all'art. 36 del decreto in rapporto all'inutilizzabilità per l'inosservanza delle garanzie difensive[60].

Pur prescrivendo tali regole processuali, la direttiva tace completamente in merito ad eventuali conseguenze derivanti dalla loro violazione: il § 1 dell'art. 14, infatti,

---

[55] Cfr. § 4.1.

[56] Sul punto, approfonditamente, G. M. RUOTOLO, *Il ruolo del consenso del sovrano territoriale nel* transborder data access *tra obblighi internazionali e norme interne di adattamento*, in *La comunità internazionale*, 2016, f. 2, p. 183 ss.; M. TORRE, sub *art. 234* bis, in *Codice di procedura commentato*, cit.

[57] Cass., Sez. VI, 28 febbraio 2023, n. 8714, non massimata.

[58] Va peraltro precisato che la cooperazione giudiziaria in materia penale, di cui all'art. 82, § 1, TFUE, si fonda sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie, basato – a sua volta – sulla fiducia reciproca e sulla presunzione relativa che gli altri Stati membri rispettino il diritto dell'Unione e, in particolare, dei diritti fondamentali dell'UE. Cfr., per tutti, CGUE, 11 novembre 2021, *Gavanozov,* in *C-852/19.*

[59] Ai sensi dell'art. 14, § 7, «[…]. Fatte salve le norme procedurali nazionali, gli Stati membri assicurano che nei procedimenti penali nello Stato di emissione siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove acquisite tramite l'O.E.I.».

[60] Sul punto, per tutti, A. CABIALE, *I limiti alla prova nella procedura penale europea,* cit., p. 260 ss.

si limita ad affermare che gli Stati membri «*shall ensure that legal remedies equivalent to those available in a similar domestic case, are applicable to the investigative measures indicated in the EIO*». Molto semplicemente, tramite una clausola di equivalenza, viene fatto rinvio gli strumenti di doglianza già predisposti nel diritto interno in relazione alle medesime attività istruttorie[61].

Senza entrare nel merito dei rimedi esperibili contro le violazioni dei diritti fondamentali, dall'esegesi delle norme che tipizzano le *exclusionary rules* si ricava un principio generale di diritto consistente nell'impossibilità di procedere ad investigazioni transfrontaliere per l'acquisizione di elementi probatori utili alle indagini disattendendo le regole di ammissibilità delle prove operanti a livello nazionale, pena l'inutilizzabilità delle informazioni raccolte[62].

In altre parole, allo stato attuale, spetta al solo diritto nazionale stabilire le regole relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale instaurato nei confronti di persone sospettate di atti criminali, di informazioni e di elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati, contraria al diritto dell'Unione (c.d. principio di autonomia procedurale).

Di qui, si potrebbe arrivare a ritenere che i risultati di indagini esperite all'estero e acquisiti in Italia per il tramite dell'O.E.I. sarebbero inutilizzabili perché ottenuti disattendendo le regole nazionali che – è bene ribadirlo – non consentono di apprendere indiscriminatamente tutti i dati comunicativi transitanti o archiviati su sistemi informatici.

Deve, tuttavia, evidenziarsi che l'obiezione non sembra essere del tutto pertinente in considerazione di quanto già evidenziato a proposito delle investigazioni esperite interamente su territorio nazionale[63]: l'atto di indagine esperito all'estero può considerarsi legittimo secondo le previsioni dell'ordinamento interno, in quanto l'acquisizione di dati sul *server* allocato in territorio straniero consiste in un atto "tipico" del processo penale nazionale, ossia l'intercettazione telematica (in caso di attività "*live*") ovvero il sequestro probatorio (nel caso di "congelamento" del *server*).

4.3. Segue: … le investigazioni sono condotte su server *allocato in Paesi* extra-*UE.*

L'ultimo caso da vagliare inerisce all'ipotesi – tutt'altro che peregrina – in cui il *server* sia allocato in Paesi *extra*-unionali.

---

[61] Sul tema, approfonditamente, E. LORENZETTO, *L'assetto delle impugnazioni*, in AA. VV., *L'ordine europeo di indagine penale*, cit., p. 157.

[62] In sostanza, l'O.E.I. deve avere ad oggetto una prova acquisibile nello Stato di emissione e deve essere eseguito in conformità di quanto previsto nello Stato di esecuzione per il compimento di un analogo atto di acquisizione probatoria, potendosi peraltro presumere il rispetto di tale disciplina e dei diritti fondamentali, salvo concreta verifica di segno contrario. Cfr. Cass., Sez. VI, 25 ottobre 2022, n. 48330, in *C.E.D. Cass.*, n. 284027.

[63] Cfr. le considerazioni effettuate a proposito acquisizioni di dati precostituiti su *server* allocato in Italia (§ 4.1).

Generalmente, allorquando occorre svolgere un'attività investigativa in uno Stato non rientrante nella "competenza" dell'Unione europea, la forma di cooperazione internazionale da impiegare è la rogatoria, secondo le previsioni di cui agli artt. 727 ss. c.p.p.[64]. Si tratta di uno strumento di assistenza giudiziaria invocabile – almeno in astratto – ogniqualvolta l'intercettazione abbia ad oggetto utenze situate in parte o del tutto in uno Stato *extra*-unionale[65].

Al fine di verificare la sua compatibilità con l'acquisizione *"live"* di comunicazioni in transito su piattaforme criptate, occorre innanzitutto soffermarsi sulla fisionomia che l'istituto della rogatoria ha assunto negli ultimi anni.

Genericamente, per *ius receptum,* la rogatoria è diventata una forma di cooperazione "residuale" cui ricorrere solo per captare conversazioni e comunicazioni "estero su estero" non transitanti su nodi italiani, ovvero effettuate senza l'ausilio dei c.d. ponti telefonici[66]. Al contrario, quando il traffico telefonico viene captato dall'Italia (a prescindere dal luogo in cui si trova l'utenza), non si delineano i presupposti della rogatoria ma del c.d. instradamento[67].

Tale tecnica investigativa consente la percezione delle comunicazioni che partono dall'Italia e sono dirette ad un'utenza estera determinata, o ad un fascio di utenze appartenenti ad un distretto geografico di cui fa parte una città situata all'estero, con possibilità di utilizzo simultaneo dei flussi telematici in luoghi e nazioni diversi ed evidenti sconfinamenti nella percezione dei contenuti comunicativi di soggetti al di fuori della giurisdizione nazionale. In questi casi, come chiarito dalla giurisprudenza di legittimità[68], non risulta necessario ricorrere alle tecniche di cooperazione internazionale

---

[64] Sull'istituto in esame, senza pretese di completezza, v. AA. VV., *Rogatorie penali e cooperazione giudiziaria internazionale*, Torino, 2003; G. DARAIO, *Le rogatorie*, in AA. VV., *Procedura penale. Teoria e pratica del processo,* diretto da G. SPANGHER-A. MARANDOLA-G. GARUTI-L. KALB, vol. IV, Torino, 2015, p. 1155 ss.; G. DELLA MONICA, voce *Rogatorie*, *Diritto* on line *2016*, in *www.treccani.it*; M.R. MARCHETTI, *L'assistenza giudiziaria internazionale,* cit., p. 60 ss.; B. PIATTOLI, voce *Rogatorie e cooperazione internazionale nel processo penale*, in *Dig. disc. pen*., Agg. III, Torino, 2005, p. 1471. Sull'istituto modificato ad opera del d.lgs. 3 ottobre 2017, n. 149, *ex multis*, E. CALVANESE, *La "nuova" assistenza giudiziaria: le rogatorie dall'estero e per l'estero*, in AA. VV., *La nuova cooperazione giudiziaria penale,* cit., p. 43 ss.; G. DI PAOLO, *Rogatorie*, in AA. VV., *Processo penale e regole europee,* cit., p. 125 ss.; EAD., *La riforma della disciplina codicistica delle rogatorie internazionali,* in *Cass. pen*., 2018, f. 7-8, p. 3431 ss.; F. RUGGIERI, *Diritto processuale e pratiche criminali*, Bologna, 2018, p. 543 ss.

[65] Sembra ormai superata la *querelle* insorta in dottrina in rapporto alla possibilità di ricorrere alla rogatoria per il compimento di atti di indagine: l'art. 727 c.p.p., così come riformato *ex* d.lgs. 149/2017, consacra definitivamente una simile possibilità.

[66] Sul tema, diffusamente, S. ALLEGREZZA-F. NICOLICCHIA, *L'acquisizione della prova all'estero e i profili transnazionali*, in AA. VV., *Diritto penale delle società*, a cura di G. CANZIO-L.D. CERQUA-L. LUPARIA, Padova, 2014, p. 1275 ss.

[67] Assai critici circa l'impiego della tecnica dell'instradamento, F. RUGGIERI, *Le intercettazioni "per instradamento" sul canale internazionale: un mezzo di ricerca della prova illegittimo,* in *Cass. pen*., 2000, p. 1062 ss.; A. GAITO, *Intercettazioni illecite, intercettazioni illegali, intercettazioni illegittime,* in AA. VV., *Le intercettazioni di conversazioni e comunicazioni. Un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti*, a cura di R.E. KOSTORIS, Milano, 2013, p. 171 ss.; F. VERGINE, *L'elemento della extraterriotorialità,* in AA. VV., *L'intercettazione di comunicazioni,* a cura di T. BENE, Bari, 2018, p. 350.

[68] In questo senso si è espressa la giurisprudenza di legittimità. Per tutti, Cass., Sez. III, 3 marzo 2016, n. 25833, in *C.E.D. Cass*., n. 267090. Per una ricostruzione dell'*iter* seguito dalla giurisprudenza, si rimanda a L. FILIPPI, sub *art. 266,* in *Codice di procedura commentato*, cit.

dal momento che l'indagine va qualificata come interna e non gestita dallo Stato straniero.

Dunque, quello che rileva ai fini della previsione delle forme di assistenza giudiziaria non è il luogo di captazione ma di acquisizione dei risultati appresi mediante intercettazione[69]: così, se gli elementi di prova si trovano all'estero ma, grazie alla tecnologia, diventa possibile apprenderli in Italia, l'indagine deve essere qualificata come "interna".

Nonostante la perimetrazione dell'istituto – almeno nella sua veste tradizionale – abbia trovato una sedimentazione pressoché stabile in dottrina e in giurisprudenza, la questione non è di facile soluzione allorquando, nell'esperimento di investigazioni transfrontaliere, gli inquirenti si avvalgono di nuovi strumenti o nuove tecniche di indagine.

In questi casi, non è affatto agevole individuare il *discrimen* tra rogatoria e instradamento, ponendosi difficoltà interpretative sia con riferimento alla verifica della necessità del ricorso alle forme di cooperazione internazionale, sia con riguardo alla tipologia di assistenza da richiedere.

Tale criticità sembra essere stata superata di recente dalla giurisprudenza di legittimità[70]: anche se con riferimento alle intercettazioni esperite per il tramite del captatore informatico – duplicando gli orientamenti già sedimentati in rapporto alle tradizionali intercettazioni itineranti espletate mediante cimici "fisiche"[71] e al meccanismo di captazione dei messaggi del tipo *Blackberry*[72] –, la Corte precisa che «[L']intercettazione ambientale a mezzo *virus* informatico installato in Italia su telefono collegato ad un gestore nazionale, non richiede l'attivazione di una rogatoria internazionale per il solo fatto che le conversazioni siano eseguite in parte all'estero, e temporaneamente registrate tramite *wifi* locale, […] atteso che la captazione ha avuto origine e si è comunque realizzata in Italia, attraverso le centrali di ricezione presso la procura della Repubblica»[73].

---

[69] Secondo R. ORLANDI, *Questioni in materia di intercettazioni di comunicazioni,* in AA. VV., *Criminalità transnazionale tra esperienze europee e risposte penali globali,* Milano, 2005, p. 320, il principio che regge il sistema della cooperazione è quello del "*locus regit actum*".

[70] Cfr. Cass., Sez. II, 22 luglio 2020, n. 29362, in *C.E.D. Cass*., n. 279815.

[71] In effetti, la Suprema Corte ha chiarito che «[L'] intercettazione di comunicazioni tra presenti eseguita a bordo di una autovettura attraverso una microspia installata nel territorio nazionale, dove si svolge altresì l'attività di captazione, non richiede l'attivazione di una rogatoria per il solo fatto che il suddetto veicolo si sposti anche in territorio straniero ed *ivi* si svolgano alcune delle conversazioni intercettate». In questo senso Cass., Sez. III, 19 gennaio 2017, n. 24305, in *C.E.D. Cass*., n. 269984. Contraria a questa impostazione è la dottrina maggioritaria. Cfr., per tutti, C. FANUELE, *La localizzazione satellitare nelle investigazioni penali*, Milano, 2019, p. 70.

[72] Come rilevato, «[…] l'acquisizione della messaggistica, scambiata mediante sistema *Blackberry*, non necessita di rogatoria internazionale quando le comunicazioni siano avvenute in Italia, a nulla rilevando che per "decriptare" i dati identificativi associati ai codici PIN sia necessario ricorrere alla collaborazione del produttore del sistema operativo avente sede all'estero». Così Cass., Sez. IV, 15 ottobre 2019, n. 49896, in *C.E.D. Cass*., n. 277949.

[73] In questo senso Cass., Sez. II, 22 luglio 2020, n. 29362, cit. Più precisamente, la Corte si è confrontata con l'intercettazione ambientale eseguita mediante captatore informatico eseguita parzialmente su territorio estero (in Canada, in particolare). In quel caso, il *malware* viene inoculato nel corso di un'indagine iniziata

La ragione di una simile impostazione deriva, secondo la Corte, dalla presa di coscienza della lentezza della procedura rogatoriale che, evidentemente, mal si concilia con la celerità delle indagini informatiche.

Una simile impostazione potrebbe trovare impiego anche nel caso delle investigazioni "*live*" esperite sulle piattaforme di comunicazioni criptate: in tali circostanze, infatti, sembra possibile ricorrere alla tecnica dell'instradamento, non dovendosi attivare la procedura rogatoriale, posto che la registrazione dei dati allocati all'estero rappresenta solamente un segmento di una più imponente attività di investigazione che, di fatto, si svolge sul territorio dello Stato. La decriptazione delle comunicazioni a seguito dello "stoccaggio" dei dati rappresenta, infatti, la fase conclusiva del più complesso *iter* esecutivo dell'attività intercettiva che, evidentemente, viene effettuata in Italia presso i *server* della procura della Repubblica.

Per converso, una simile conclusione non può essere raggiunta nel caso in cui l'investigazione abbia ad oggetto l'acquisizione dei dati giacenti sui *server* situati in Paesi *extra*-unionali: in questi casi – allorquando la captazione non ha ad oggetto flussi comunicativi in transito – l'apprensione delle informazioni utili all'accertamento dei fatti in un processo penale instaurato in Italia deve avvenire per il tramite della rogatoria internazionale[74].

Unica eccezione alla regola ricorre nel caso in cui il titolare del dato ceda spontaneamente i dati ottenuti mediante un'investigazione interna: come anche chiarito dalla giurisprudenza di legittimità, «[…] le informazioni e gli atti trasmessi autonomamente dall'autorità giudiziaria di uno Stato estero sono utilizzabili nel procedimento penale, non essendo, in tali casi, applicabile in via estensiva o analogica la disciplina speciale prevista dall'art. 729, comma 1, c.p.p. per le rogatorie dall'estero»[75].

5. Proposte.

Alla luce di quanto esposto, possono trarsi delle considerazioni di carattere sistemico che offrono nuovi spunti di riflessione per il giurista.

La prima non può che essere rivolta ai "pratici", ossia a coloro che ricorrono a sofisticate tecniche di indagine quali strumenti principali per l'esecuzione delle investigazioni. Posta la loro imprescindibilità nell'accertamento e nella repressione delle più gravi ed evolute forme di criminalità, non è il loro impiego ad essere oggetto di critica, ma l'abuso, ossia il ricorso smodato a tali tipologie di indagine. Sembra necessario – prima di ogni cosa – immaginare tali tecniche come una *extrema ratio*, cui ricorrere

---

sul territorio nazionale in uso a due indagati che, nel tempo coperto dall'autorizzazione giurisdizionale, si sono recati all'estero portando con sé l'apparecchio infetto. In sostanza, tali utenze vengono utilizzate sia in territorio italiano sia in quello canadese, pur essendo collegate ad un gestore italiano. Per un commento della pronuncia in esame, per tutti, P. MAGGIO, *Intercettazioni* no limits: il *captatore informatico "per instradamento"*, in *Proc. pen. giust.*, 2021, f. 2, p. 448 ss.

[74] In questo senso anche Cass., Sez. VI, 20 aprile 2021, n. 18907, in *C.E.D. Cass.*, n. 281819.

[75] Cass., Sez. I, 16 giugno 2022, n. 354, in *C.E.D. Cass.*, n. 28386.

allorquando le altre modalità di indagine risultano inefficaci allo scopo perseguito: l'uso "parsimonioso" delle strumentazioni ad alto potenziale intrusivo, il c.d. *hacking* etico, potrebbe rappresentare un primo passo per il raggiungimento dell'equilibrio tra sicurezza e diritti individuali[76].

La seconda considerazione non può che avere come referente chi il sistema politico–criminale lo governa e lo plasma secondo le esigenze contingenti. Sembra indispensabile prevedere una regolamentazione dei servizi di comunicazione cifrata attraverso l'aggiornamento del Codice delle comunicazioni elettroniche[77]. L'obiettivo è fornire un elenco di piattaforme criptate autorizzate a rilasciare il servizio, i cui gestori si impegnano a collaborare con le autorità di *law enforcement* per sviluppare soluzioni che permettano di individuare e bloccare gli utenti che utilizzano le piattaforme per commettere reati.

Sotto il profilo più propriamente processuale – poiché non si può considerare *a priori* incostituzionale ogni strumento o tecnica di indagine innovativa attraverso cui condurre le indagini[78] –, si ritiene indispensabile introdurre una disciplina atta a regolamentare le nuove forme di indagine ad alto potenziale tecnologico, tenendo conto del bilanciamento tra i vari interessi che possono venire in contrasto.

Precisamente, non essendo ipotizzabile lasciare alla disponibilità degli inquirenti la scelta di ricorrere indiscriminatamente a nuove tecniche di indagine e nemmeno legittimare il loro impiego in sede giurisprudenziale attraverso interpretazioni estensive in una materia governata da un rigido principio di tassatività, si avverte l'esigenza di un intervento del legislatore, chiamato a tipizzare il complesso di attività esperibili attraverso di nuove tecniche investigative digitali, di modo tale da rendere le limitazioni alle prerogative individuali "tollerabili" in una società democratica.

Nonostante la normativizzazione delle tecniche di investigazioni digitale rappresenti un baluardo ineludibile contro gli arbìtri del giudicante, anche le modalità di intervento legislativo non risultano di immediata soluzione.

Prima facie, posta la sussumibilità dell'attività investigativa "*live*" esperita su piattaforme criptate alle previsioni di cui all'art. 266 *bis* c.p.p., si potrebbe prevedere una modifica della disciplina delle intercettazioni informatiche o telematiche attraverso l'innesto di un nuovo comma 1 *bis* alla norma *de qua*, così da tipizzare le forme di captazioni di comunicazioni su larga scala quali nuove "tecniche" attraverso cui esperire un tradizionale mezzo di ricerca della prova.

Se questa fosse la soluzione, sarebbe anche doveroso procedere all'adeguamento al complesso disciplinare delle intercettazioni, intervenendo sugli artt. 267, 269, 270 e 271 c.p.p., nonché sul dettato di cui all'art. 89 disp. att. c.p.p.

---

[76] Nel senso di garantire forme di "hackeraggio etico", cfr. A. HENSCHKE, *Ethics in an Age of Surveillance personal information and virtual identities,* Cambridge University Press, 2017, p. 43 ss.

[77] D. lgs. 1 agosto 2003, n. 259.

[78] In questo senso, C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007, p. 151. Ma già V. GREVI, *Insegnamenti, moniti e silenzi della Corte Costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost*., 1973, p. 341.

In quest'ottica, sarebbe auspicabile: a) circoscrivere i presupposti per autorizzare le intercettazioni di comunicazioni su larga scala, limitando il ricorso a tale forma captativa ai soli procedimenti relativi ai reati di cui agli artt. 51, comma 3 *bis* e 3 *quater* e 407, comma 2, lett. a, c.p.p.; b) rafforzare il contenuto del decreto autorizzativo del g.i.p., attraverso la precisazione delle ragioni che rendono necessario il ricorso a tale forma captativa; c) prevedere la distruzione obbligatoria del materiale "irrilevante" per le indagini; d) estendere la portata della sanzione dell'inutilizzabilità delle intercettazioni di comunicazioni su larga scala in procedimenti diversi, magari riservando l'eccezione ai soli casi per i quali le informazioni risultino rilevanti e indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza; e) potenziare le procedure atte a garantire la corretta acquisizione dei dati digitali per attestarne la genuinità e l'immodificabilità.

Per altro verso, si potrebbe scegliere di "ammodernare l'esistente" attraverso un intervento legislativo additivo delle norme disciplinanti i singoli mezzi di ricerca della prova: in questo senso, l'innesto sarebbe funzionale a tipizzare le differenti attività – osservazione, accesso, acquisizione e captazione – che scaturiscono dalle investigazioni sulle piattaforme criptate.

Di qui, sulla base delle modifiche già operate dalla l. 18 marzo 2008, n. 48, per adeguare le investigazioni "fisiche" alla dimensione virtuale, si potrebbe prevedere un'estensione della disciplina già operante in materia di ricerca e apprensione dei dati informatici a fini di prova alle c.d. acquisizioni di dati su larga scala, innovando le disposizioni in materia di ispezioni informatiche (art. 244, comma 2, c.p.p.), perquisizioni informatiche (art. 247, comma 1 *bis*, c.p.p.), sequestro probatorio presso gli *Internet Service Providers* (art. 254 *bis* c.p.p.) e intercettazioni telematiche (art. 266 *bis*, comma 1, c.p.p.);

Non vanno, tuttavia, sottaciuti i rischi che possono derivare da un simile approccio "attivista", fondato, cioè, sulla convinzione per cui la positivizzazione dell'istituto rappresenti la soluzione ai mali del sistema.

Come sempre accade quando il processo penale si confronta con i nuovi ritrovati della scienza e della tecnica, il pericolo è di intervenire su una materia già diventata obsoleta, perché – si sa – i tempi delle riforme non coincidono con la velocità propria del progresso e dell'evoluzione tecnologica, condannando la legge ad una obsolescenza precoce.

Al fine di arginare simili *pericula*, si potrebbe propendere per l'introduzione di un nuovo mezzo di ricerca della prova (accesso e acquisizione di *big data* su sistemi informatici o telematici, potrebbe chiamarsi) per regolare le attività di accesso, osservazione e acquisizione di dati e informazioni rinvenuti sui nuovi spazi virtuali: in questi casi, non sarebbe tipizzato lo strumento con cui condurre le indagini informatiche quanto piuttosto le regole cui ricorrere ogni qual volta si proceda ad attività di sorveglianza occulta e continuativa da remoto, predisponendo le garanzie fondamentali che devono essere sempre riconosciute all'indagato e ai soggetti terzi occasionalmente coinvolti, a prescindere dalla tecnica investigativa impiegata.

In altre parole, l'obiettivo potrebbe essere quello di introdurre una nuova categoria probatoria, con la quale verrebbero individuati i "casi" e i "modi"

dell'ingerenza nella sfera privata degli individui, così da ritenere il sacrificio dei diritti inviolabili assolutamente rispettoso del principio di stretta legalità e del principio di proporzione.

Infine, in una prospettiva sovranazionale, sarebbe auspicabile la predisposizione di una normativa uniforme sulla circolazione dei dati digitali.

Più concretamente, nell'ambito della Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (c.d. Regolamento *E-Evidence*)[79], si potrebbe prevedere l'introduzione di una procedura volta a facilitare lo scambio delle informazioni acquisite all'estero (in Paesi *intra*-unionali) per il tramite delle investigazioni esperite mediante nuove tecniche di indagine e, al contempo, predisporre una norma costruita sul modello del dettato di cui art. 270 c.p.p. italiano, individuando limiti e prospettive comuni per acquisire risultati di captazioni in Stati diversi da quelle per cui sono state autorizzate.

Nonostante gli sforzi profusi per tentare di fornire adeguati rimedi ai problemi posti dall'impiego di sempre più sofisticate tecniche investigative, l'indagine non consente di addivenire ad una soluzione condivisa. Rispettando i crismi propri di qualsivoglia ricerca, l'analisi lascia ancora imbattute e inesplorate diverse rotte. L'irrefrenabile velocità con cui gli strumenti investigativi si evolvono apre, infatti, la strada all'impiego di ulteriori e ancora più sofisticati metodi di indagini (intelligenza artificiale, droni, *robot* e, soprattutto, il metaverso)[80] che sono destinati a comprimere – inevitabilmente – fondamentali diritti degli individui, nel frattempo privati di adeguate forme di tutela nell'assenza di una normativa che li contempli. Ecco allora, che le riflessioni condotte non possono che rappresentare il nuovo punto di partenza per un sistema processuale penale "informatizzato" ancora allo stato embrionale.

---

[79] Si tratta della Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, COM (2018) 225 final, 17 aprile 2018. Sulla proposta, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento* e-evidence, in *Cass. pen.*, 2019, p. 1340 ss.; F. RUGGIERI, *Il Protocollo 16 alla CEDU in vigore dal 1° agosto 2018. La Proposta per l'ordine europeo di conservazione o produzione della prova digitale*, in *Cass. pen.*, 2018, p. 2660. Mette in risalto la necessità di procedere celermente all'adozione del Regolamento, D. CURTOTTI, *Indagini* hi-tech, *spazio* cyber, *scambi probatori tra Stati e* Internet provider service *e "Vecchia Europa": una normativa che non c'è (ancora),* in *Dir. pen. proc.*, 2021, p. 745. Per dovere di completezza, si segnala che, a distanza di oltre cinque anni dall'approvazione della Proposta, il Consiglio dell'UE, con un comunicato stampa del 25 gennaio 2023, conferma l'accordo con il Parlamento europeo sulla necessità di adottare nuove norme per migliorare l'accesso transfrontaliero alle prove elettroniche.

[80] E, *The metaverse,* in *Digital evidence and Electronic Signature Law Review,* n. 19, 2022, p. 1.

Editore

ASSOCIAZIONE
"PROGETTO GIUSTIZIA PENALE"