OEI E MESSAGGI DIGITALI GIÀ ACQUISITI ALL'ESTERO

Riflessioni a partire dal caso Sky ECC [*]

di Marcello Daniele

Nel caso Sky ECC, i problemi tipici della raccolta transnazionale delle prove attraverso l'ordine europeo di indagine penale si sono incrociati con la complessità delle indagini informatiche. In un contesto così intricato, diviene ancora più difficile individuare il corretto punto di equilibrio fra la tutela dei diritti fondamentali e la salvaguardia delle esigenze investigative. La sfida è consentire agli organi inquirenti di svolgere i loro compiti evitando di compromettere in modo irreparabile il diritto alla riservatezza, le garanzie difensive e l'attendibilità delle prove acquisite.

1. Il caso *Sky ECC*.

La tecnologia informatica offre alla criminalità strumenti sempre più efficaci e sofisticati. Emblematico, in questo senso, il caso *Sky ECC*, relativo ad una piattaforma di messaggistica che aveva consentito agli esponenti di alcune organizzazioni dedite al traffico internazionale di stupefacenti di comunicare tramite dispositivi dotati di sistemi di crittografia (i c.d. "criptofonini").

[*] Testo della relazione, ampliata e corredata di note, svolta nell'ambito del corso *La cooperazione giudiziaria in materia penale nel quadro dei processi europei di digitalizzazione della giustizia* (Napoli, 9-11 dicembre 2024), organizzato dalla Scuola Superiore della Magistratura.

Editore Associazione "Progetto giustizia penale" | via Festa del Perdono 7, 20122 Milano
c/o Università degli Studi di Milano, Dipartimento di Scienze Giuridiche "Cesare Beccaria"
redazione@sistemapenale.it

Tramite una complessa operazione di *hacking*, le autorità giudiziarie francesi erano riuscite a venire in possesso dei messaggi scambiati attraverso la piattaforma. Trattandosi di prove rilevanti anche ai fini di taluni procedimenti italiani, le nostre autorità giudiziarie ne avevano ottenuto la trasmissione da parte delle autorità francesi tramite l'ordine europeo di indagine penale (OEI)[1].

Come è facile immaginare, la loro utilizzabilità nel contesto del nostro sistema è tutt'altro che pacifica. Su questo terreno, la dialettica fra le garanzie processuali e le esigenze repressive si fa più che mai serrata. Ed è un'ardua impresa, come vedremo, salvaguardare pienamente le prime senza rischiare di pregiudicare le seconde.

2. Le modalità di acquisizione dei messaggi digitali già ricevuti dal proprio destinatario: un ripensamento.

Non ci sono dubbi che comunicazioni come quelle venute in gioco nel caso *Sky ECC*, trasmesse attraverso sistemi e dispositivi informatici, abbiano natura digitale. Meno chiaro, invece, è come esse dovrebbero essere acquisite a livello processuale.

Laddove si verifichi nel momento stesso in cui i messaggi vengono trasmessi, la captazione può farsi senz'altro rientrare nel paradigma delle intercettazioni c.d. telematiche (art. 266 *bis* s. c.p.p.).

Le incertezze aumentano, invece, qualora l'acquisizione avvenga dopo che siano già stati trasmessi, nel momento in cui si trovino ormai nelle memorie dei dispositivi informatici del mittente o del destinatario, oppure nei *server* dei fornitori dei servizi di messaggistica (*service provider*).

A quest'ultimo riguardo, in precedenza si era sviluppata l'interpretazione secondo la quale, essendo i messaggi già stati ricevuti dal proprio destinatario, sarebbe venuto meno il rischio di una loro apprensione da parte di estranei, con la conseguenza che essi avrebbero dovuto essere qualificati come meri documenti. E, in quanto prove precostituite, la loro raccolta non avrebbe avuto bisogno di particolari garanzie. Si riteneva sufficiente la loro riproduzione fotografica[2], anche effettuata dalla polizia a prescindere dall'autorizzazione di un'autorità giudiziaria[3].

Le cose sono cambiate grazie ad una sentenza della Corte costituzionale[4], che ne ha finalmente riconosciuto la natura digitale con tutte le conseguenze che dovrebbero derivarne in merito alle modalità di acquisizione[5].

---

[1] Ossia lo strumento di raccolta transnazionale delle prove di cui si sono dotati gli Stati dell'Unione Europea con la Direttiva 41/2014 del 3 aprile 2024, recepita nel nostro sistema con il d.lgs. 21 giugno 2017, n. 108.

[2] Si pensi agli *screenshot* degli smartphone, tali da riportare le conversazioni avvenute su *whatsapp* o su analoghi sistemi di messaggistica.

[3] Così Cass., sez. VI, 21 settembre 2023, n. 38678; Id., sez. V, 14 febbraio 2023, n. 24824; Id., sez. VI, 12 novembre 2019, n. 1822.

[4] Cfr. Corte cost., 7 giugno 2023, n. 170, relativa ad un conflitto di attribuzione tra poteri dello Stato sorto in rapporto alla possibilità per l'autorità giudiziaria di acquisire talune comunicazioni elettroniche del senatore Matteo Renzi in assenza di un'autorizzazione da parte del Senato della Repubblica.

[5] Sulla raccolta delle prove digitali cfr., in generale, M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, pp. 283 s.; G. DI PAOLO, *Prova informatica (diritto processuale penale)*, in *Enc. dir., Annali*, vol. VI,

Il fatto che si tratti di messaggi già ricevuti dal proprio destinatario – hanno osservato i giudici costituzionali – non fa venire meno l'esigenza di proteggerne la riservatezza: «degradare la comunicazione a mero documento quando non più *in itinere*» è una soluzione che finisce per azzerare le garanzie previste dall'art. 15 Cost. in rapporto alla libertà e alla segretezza della corrispondenza, se si considera che, in relazione alle «comunicazioni operate tramite posta elettronica e altri servizi di messaggistica istantanea», «all'invio segue immediatamente – o, comunque sia, senza uno iato temporale apprezzabile – la ricezione».

La tutela costituzionale - conclude la Corte - verrebbe meno solo quando, «per il decorso del tempo», il messaggio «abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento storico»[6].

Grazie a questo apprezzabile ripensamento, si sta consolidando l'idea, pure nella giurisprudenza della Corte di cassazione, che i messaggi digitali, anche se già ricevuti dal loro destinatario, possano essere acquisiti solo in forza di un atto motivato dell'autorità giudiziaria, così come richiesto dall'art. 15 comma 2 Cost.[7].

3. Mappatura delle garanzie nazionali.

In quanto prove digitali, i messaggi di cui si discute vanno, dunque, maneggiati dalle autorità giudiziarie osservando certe cautele, capaci di preservarne il valore conoscitivo e, al contempo, di limitare la compressione del diritto alla riservatezza suscettibile di derivare dalla loro acquisizione.

Stiamo parlando di garanzie che possono assumere varie conformazioni, e che si possono così individuare.

a) ***Controllo giurisdizionale***, che potrebbe essere:

- Preventivo, tramite l'autorizzazione di un giudice allo svolgimento delle attività istruttorie;
- oppure successivo, tramite la previsione di un mezzo di impugnazione, oppure di un'inutilizzabilità rilevabile dal giudice chiamato ad avvalersi della prova.

Entrambe le tipologie di controllo hanno vantaggi e svantaggi.

Il controllo preventivo può evitare fin dall'inizio la compressione del diritto alla riservatezza; al contempo, però, è più limitato, perché, essendo per l'appunto anteriore all'attività istruttoria, per definizione non può estendersi alle modalità con cui la prova è stata raccolta.

Giuffrè, 2013, pp. 736 s.; M. PITTIRUTI, *Digital evidence e procedimento penale*, Giappichelli, 2018, pp. 33 s.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, pp. 49 s.

[6] Attualità che, peraltro, dovrebbe «presumersi, sino a prova contraria, quando si discuta di messaggi scambiati a una distanza di tempo non particolarmente significativa rispetto al momento in cui dovrebbero essere acquisiti», specie laddove essi siano «ancora custoditi in dispositivi protetti da codici di accesso»: Corte cost., 7 giugno 2023, n. 170, § 4.4.

[7] V., ad esempio, Cass., sez. VI, 20 novembre 2024, n. 1269; Id., sez. VI, 28 ottobre 2024 n. 39548; Id., sez. II, 15 maggio 2024, n. 25549.

Il controllo successivo, dal canto suo, interviene dopo che la compressione del diritto alla riservatezza è avvenuta, ma può estendersi anche alle modalità di raccolta della prova.

La presenza di un controllo giurisdizionale dell'uno o dell'altro tipo, in ogni caso, costituisce una forma di protezione ineludibile. È vero che gli artt. 14 e 15 Cost. richiedono, ai fini della limitazione del diritto alla riservatezza, un atto motivato dell'"autorità giudiziaria", espressione che designa anche il solo pubblico ministero. L'esigenza di un controllo giurisdizionale perlomeno successivo, nondimeno, viene ricavato dalla Corte europea dei diritti dell'uomo sulla base della clausola della "necessità in una società democratica" della restrizione prevista dall'art. 8 § 2 CEDU[8].

Nè va dimenticato che la Corte di giustizia dell'Unione Europea ha esplicitamente affermato che talune operazioni istruttorie richiedono un controllo giurisdizionale preventivo: l'acquisizione dei dati esterni alle comunicazioni (c.d. "dati di traffico")[9] e, più di recente, proprio l'acquisizione dei dati contenuti nei telefoni cellulari[10] .

b) Proporzionalità, che contribuisce a definire l'oggetto del controllo giurisdizionale, e si concretizza in una serie di presupposti per lo svolgimento dell'atto istruttorio:

- l'esistenza di una giustificazione fattuale[11];
- la stretta necessità, che consiste nell'assenza di misure meno invasive capaci di ottenere il medesimo risultato;
- l'attinenza del procedimento a reati di una certa gravità.

c) Obbligo di impiegare le migliori tecniche informatiche, capaci di impedire la manipolazione delle prove digitali, assicurandone la valenza conoscitiva.

d) Contraddittorio tecnico, che potrebbe essere:

- di tipo contestuale, attraverso la formazione della prova digitale nello scontro dialettico delle parti, sul modello della procedura prevista dall'art. 360 c.p.p. in rapporto agli accertamenti tecnici non ripetibili;
- oppure posticipato, con la possibilità per le parti di interloquire, anche con l'ausilio di esperti, sulle modalità con cui la prova è stata raccolta, e sul conseguente valore conoscitivo che essa è destinata a possedere.

Idealmente parlando, il contraddittorio contestuale sarebbe la soluzione da preferire, considerati i rischi di alterazione a cui le prove digitali sono sottoposte. Ma purtroppo spesso esso non è praticabile: magari perché al momento della raccolta della prova non esiste ancora un indagato noto; oppure perché vi è una situazione di urgenza,

[8] V., fra le molte, Corte eur., 4 dicembre 2015, *Roman Zakharov c. Russia*, § 257 s. (sulle intercettazioni), e Id., 27 settembre 2018, *Bracci c. Italia*, § 38 s. (sulle perquisizioni).
[9] V. Corte giust., 2 marzo 2021, C-746/18, *HK*, § 46 s.
[10] Cfr. Corte giust., 4 ottobre 2024, C-548/21, *CG*, § 78 s.
[11] Si pensi, quanto al nostro sistema, al "fondato motivo" richiesto per le perquisizioni, o ai "gravi indizi di reato" postulati per le intercettazioni.

che rende inevitabile raccogliere immediatamente la prova senza attendere l'intervento della difesa.

e) Catena di custodia, che si identifica nella documentazione predisposta per certificare lo svolgimento delle operazioni istruttorie.

Essa dovrebbe indicare in che modo le prove digitali sono state raccolte e conservate dall'inizio alla fine della loro filiera acquisitiva, nei vari passaggi di mano dagli organi investigativi al giudice, in modo da mettere gli interessati nelle condizioni di individuare eventuali manipolazioni del loro contenuto[12].

Si tratta di una garanzia servente, che stimola l'impiego delle migliori tecniche di raccolta e di conservazione delle prove digitali, ma che concettualmente va tenuta distinta da quest'ultimo. È possibile, infatti, che l'acquisizione delle prove sia avvenuta in modo corretto, ma non sia stata adeguatamente documentata; o, al contrario, che siano state fedelmente riprodotte delle operazioni istruttorie effettuate sulla base di tecniche informatiche fallaci[13].

f) Inutilizzabilità, la quale, come si accennava, presuppone un controllo giurisdizionale successivo, e può verificarsi, a seconda dei casi:

- per la mancanza di determinati presupposti per l'adozione degli atti istruttori volti a raccogliere le prove digitali:
- oppure per la violazione delle modalità di raccolta previste dalla legge.

g) Valutazione motivata, che si identifica nel dovere del giudice di esplicitare le ragioni per cui le prove digitali sono state valutate in un certo modo, anche alla luce delle modalità con cui sono state raccolte.

Tale onere argomentativo, che discende anche dagli artt. 14 e 15 Cost., come è facile intuire cresce tanto più quanto più le prove siano state acquisite senza osservare pienamente le altre garanzie (salvo, ovviamente, che le prove debbano essere dichiarate inutilizzabili).

Conviene, a questo punto, ricordare brevemente in che modo la legge abbia modulato queste forme di tutela a livello nazionale, per poi comprendere come esse siano suscettibili di variare quando - come nel caso *Sky ECC* - le operazioni istruttorie assumano valenza sovranazionale.

---

[12] Cfr. S. SIGNORATO, *Le indagini digitali*, cit., pp. 140 s.

[13] Si veda L. BARTOLI, *La catena di custodia del materiale informatico: soluzioni a confronto*, in *Anales de la Facultad de derecho*, f. 33, 2016, p. 147.

È possibile darne una rappresentazione nel modo che segue, sia pure con qualche approssimazione e senza pretesa di esaustività[14].

GARANZIE NAZIONALI	Autorizzazione da parte di un giudice (controllo giurisdiz. preventivo)	Impugnazione (controllo giurisdiz. successivo)	Proporzionalità	Uso delle migliori tecniche informatiche	Contraddittorio tecnico contestuale o posticipato	Catena di custodia	Inutilizzabilità (controllo giurisdiz. successivo)	Valutazione motivata
Perquisizioni informatiche		art. 252 *bis* c.p.p.	art. 247 c. 1 *bis* c.p.p.	art. 247 c. 1 *bis* c.p.p.	artt. 360, 359, 501 c.p.p.	artt. 357, 373 c.p.p.		artt. 192, 546, 533 c.p.p.
Sequestri informatici		art. 257 c.p.p.	artt. 253, 254 c.p.p.	art. 259 c. 2, 260 c. 2 c.p.p.	artt. 360, 359, 501 c.p.p.	artt. 357, 373, 259 e 260 c.p.p.		artt. 192, 546, 533 c.p.p.
Intercettazioni telematiche	art. 267 c.p.p.		art. 266, 266 *bis*, 267 c.p.p.		art. 268 c. 6 s. c.p.p.	artt. 269, 89 disp. att. c.p.p.	art. 271 c.p.p.	artt. 192, 546, 533 c.p.p.

4. La raccolta dei messaggi digitali da parte delle autorità francesi nel caso *Sky ECC*.

Rispetto alla raccolta delle prove digitali in ambito nazionale, la raccolta dei messaggi nel caso *Sky ECC* presentava almeno due livelli di complicazione ulteriore.

Le attività istruttorie che avevano portato all'acquisizione dei messaggi in Francia erano consistite in sofisticate operazioni di *hacking* informatico avvenute in più tempi, così sintetizzabili nei loro passaggi essenziali:

(*i*) intercettazione, registrazione e trascrizione delle comunicazioni transitate attraverso i *server* del *service provider*, da cui erano emerse, tra l'altro, informazioni relative ai dispositivi telefonici utilizzati, e che avevano consentito di captare tutta una serie di messaggi scambiati in forma crittografata;

(*ii*) inserimento di captatori informatici all'interno dei *server*, che avevano permesso di individuare le chiavi di decriptazione grazie alle quali la polizia francese era stata in grado di decodificare i messaggi già raccolti e anche quelli acquisiti successivamente;

(*iii*) sequestro e copia forense dei *server*, il cui contenuto era stato decriptato così da arrivare a creare un archivio di comunicazioni decodificate[15].

Si era trattato, dunque, di operazioni a natura mista, non classificabili in un singolo mezzo di mezzo di ricerca della prova: il che già di per sè ne rendeva non semplice l'inquadramento giuridico.

---

[14] Allo stato è pendente in Parlamento il d.d.l. S-806, il quale mira ad introdurre un nuovo art. 254 *ter* c.p.p. che, fra l'altro, richiederebbe un'autorizzazione giurisdizionale preventiva al fine del sequestro di dispositivi e sistemi informatici: v. F.R. DINACCI, *Modi acquisitivi della messaggistica chat o e-mail: verso letture rispettose dei principi*, in *Arch. pen. online*, f. 1, 2024, pp. 13 ss.; O. MURRO, *Prospettive in tema di sequestro dello smartphone: le novità approvate dal Senato*, in *Dir. pen. proc.*, 2024, pp. 1621 ss.

[15] Per una ricostruzione di quanto avvenuto si veda la *Memoria per l'udienza delle Sezioni unite penali* del 29 febbraio 2024, in questa *Rivista*, 1° marzo 2024, pp. 23 s.

Un'altra difficoltà era legata al fatto che le autorità francesi non avevano agito su impulso delle autorità italiane, ma avevano proceduto all'acquisizione dei messaggi di propria iniziativa. La loro raccolta, dunque, era avvenuta esclusivamente sulla base delle regole francesi (*lex loci*), senza tenere conto delle regole italiane (*lex fori*). Ne era risultata, in questo modo, capovolta la regola normalmente operante per la raccolta transnazionale delle prove, secondo la quale si dovrebbe osservare la *lex fori*, salvo il rispetto dei principi fondamentali della *lex loci*[16].

5. Come acquisire i messaggi nei processi italiani?

A quali condizioni, dunque, messaggi così raccolti all'estero potrebbero essere ritenuti utilizzabili nei processi italiani?

La risposta al quesito ha richiesto l'intervento di ben due sentenze delle Sezioni Unite della Corte di cassazione[17]. Senza dimenticare che vicende analoghe a quelle di *Sky ECC* hanno portato a pronunciarsi anche la Corte di giustizia dell'Unione Europea[18] e la Corte europea dei diritti dell'uomo[19], nonchè le Corti supreme di diversi Stati nazionali[20].

6. La critica alla tesi dell'acquisizione libera *ex* artt. 234-234 *bis* c.p.p.

Avendo a che fare con messaggi digitali già autonomamente raccolti dalle autorità francesi, ci si potrebbe chiedere se le autorità italiane avrebbero potuto acquisirli prescindendo dall'impiego dell'OEI.

Come hanno posto in rilievo anche le Sezioni Unite, la risposta è da ritenersi negativa. In primo luogo, per la ragione che, come si è detto, la raccolta dei messaggi non avrebbe potuto essere ricondotta allo schema dell'acquisizione dei documenti, basato sulla mera allegazione a favore del giudice chiamato a valutarne il peso conoscitivo (artt. 234, 495 comma 3, 515 c.p.p.).

Neppure poteva venire in gioco l'art. 234 *bis* c.p.p.[21], che, quando si ha a che fare con prove precostituite, è stato concepito proprio per evitare il ricorso agli strumenti di

---

[16] Si pensi all'art. 9 § 2 direttiva 41/2014, in base al quale «l'autorità di esecuzione si attiene alle formalità e alle procedure espressamente indicate dall'autorità di emissione», «sempre che tali formalità e procedure non siano in conflitto con i principi fondamentali del diritto dello Stato di esecuzione».

[17] Cfr. Cass., sez. un., 29 febbraio 2024, n. 23755, *Gjuzi*, e n. 23756, *Giorgi*, in questa *Rivista*, con nota di M. DANIELE, *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini*.

[18] Si veda Corte giust., 30 aprile 2024, C-670/22, *MN*, § 69 s., relativa alla piattaforma *Encrochat* (un servizio di messaggistica simile a *Sky ECC*).

[19] V. Corte eur., 26 settembre 2023, *Yuksel Yalçinkaya c. Turchia*, § 302 s.

[20] Cfr., ad esempio, in rapporto alla Suprema Corte federale tedesca, T. WAHL, *Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases*, in *eucrim.eu*, 19 May 2022. V. anche la decisione della Corte di cassazione francese dell'11 ottobre 2022.

[21] Ai sensi del quale «è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare».

cooperazione giudiziaria, dettando una disciplina alternativa e incompatibile con quella dettata in tema di OEI[22].

Nel nostro caso, consistendo i messaggi in «dati informatici» non «disponibili al pubblico», sarebbe servito il consenso all'acquisizione da parte del legittimo titolare: il quale, però, non si sarebbe potuto identificare con l'autorità straniera, da considerare come mera «detentrice qualificata» di quei dati «a fini di giustizia»[23].

Si aggiunga che la direttiva 41/2014 è esplicita nell'affermare che l'OEI va utilizzato anche ai fini dell'acquisizione delle prove «già in possesso» delle competenti autorità dello Stato di esecuzione[24].

Né si poteva invocare lo strumento dello "scambio spontaneo" di informazioni fra le autorità giudiziarie di Stati diversi. Per quanto risponda ad una consolidata prassi volta a semplificare le operazioni istruttorie, quest'ultimo è formalmente previsto solo in rapporto alle rogatorie in forza dell'art. 7 della Convenzione di assistenza giudiziaria del 29 maggio 2000[25], integralmente sostituita dalla direttiva 41/2014 nei rapporti fra gli Stati che hanno recepito l'OEI[26].

Andava escluso, insomma, che i messaggi, sebbene già raccolti in modo autonomo dalle autorità francesi, fossero per ciò solo automaticamente ammissibili nei processi italiani, come se si trattasse di documenti[27].

7. La via dell'equivalenza con le regole nazionali in tema di circolazione delle prove fra procedimenti diversi.

Venendo in gioco l'OEI, non va dimenticato il c.d. principio di equivalenza, in base al quale le prove dovrebbero essere acquisite all'estero con le stesse forme e garanzie che, ai sensi della legislazione italiana, varrebbero ai fini dello svolgimento dei medesimi atti istruttori in un caso interno analogo[28].

Le implicazioni di questo principio sono più difficili da cogliere quando, come nel caso di cui ci occupiamo, le prove siano state già autonomamente raccolte all'estero prima dell'emissione dell'OEI, e quindi senza tenere in considerazione il diritto nazionale. In situazioni del genere, se il requisito dell'equivalenza venisse inteso in

[22] Cfr. la sentenza *Gjuzi*, § 6 s, e la sentenza *Giorgi*, § 9 s. In senso analogo v. S. SIGNORATO, *Indagini e prove digitali*, in *Riv. dir. proc.*, 2024, pp. 1171 ss.

[23] V. Cass., sez. VI, 26 ottobre 2023, n. 44154, § 2.3.

[24] *Considerando* 7 e artt. 1 § 1 e 10 § 2 *a*. Lo presuppongono pure gli artt. 2 comma 1 lett. *a* e 9 comma 5 lett. *a* d.lgs. n. 108 del 2017.

[25] In base al quale «le autorità competenti degli Stati membri possono procedere ad uno scambio di informazioni, senza che sia presentata una richiesta a tal fine». Nello stesso senso, si veda l'art. 9 del d.lgs. 5 aprile 2017, n. 52, che ha trasposto la Convenzione.

[26] Si veda l'art. 34 § 1 direttiva 41/2014.

[27] Ciò, peraltro, varrebbe anche nei confronti delle prove spontaneamente trasmesse ai sensi del citato art. 7 conv. ass. giud. 2000, il quale non potrebbe essere utilizzato per avallare accordi informali volti ad eludere le garanzie che dovrebbero assistere la cooperazione giudiziaria.

[28] Art. 6 § 1 *b* direttiva 41/2014; art. 27 comma 1 d.lgs. 108/2017.

modo troppo rigido, le prove rischierebbero di essere sempre inutilizzabili nei processi italiani, con il rischio di pregiudicare l'accertamento delle responsabilità penali.

A questo riguardo, la direttiva 41/2014 e il d.lgs. 108/2017 non offrono nessuna indicazione. A livello interno, la questione è lambita dall'art. 78 disp. att., relativo all'acquisizione della «documentazione di atti di un procedimento penale compiuti da autorità giudiziaria straniera».

Vi si prevede, al comma 1, che gli atti istruttori compiuti dalle autorità straniere possono essere acquisiti nei procedimenti penali nazionali «a norma dell'articolo 238 del codice»: vale a dire, delle norme che, in ambito interno, regolano la circolazione delle prove da un procedimento penale ad un altro.

Per quanto siano state concepite in riferimento alle rogatorie, nulla vieta di estendere le prescrizioni dell'art. 78 disp. att. anche all'OEI. Ed è quello che hanno ritenuto di fare le Sezioni Unite nel caso *Sky ECC*, le quali hanno calibrato l'applicazione del principio di equivalenza con i casi interni analoghi parametrandolo in rapporto non alla disciplina nazionale della "formazione", ma, per l'appunto, a quella della "circolazione" delle prove fra procedimenti diversi evocata dall'art. 78 disp. att.[29].

In questo modo, la Corte di cassazione ha affermato che, ai fini della loro spendibilità nei processi italiani, i messaggi avrebbero dovuto essere raccolti da parte delle autorità straniere assicurando il medesimo livello di garanzia previsto dall'art. 238 c.p.p., nonché dall'art. 270 c.p.p., relativo alla circolazione delle intercettazioni fra i procedimenti nazionali: il quale, sebbene non espressamente richiamato, poteva ritenersi applicabile in virtù della logica sottesa all'art. 78 disp. att.[30].

È un approccio ha sollevato varie obiezioni, le quali, però, non mi sembrano irresistibili.

7.1. Prima obiezione*: divieto di svolgere in Italia le operazioni istruttorie francesi.*

Si è affermato, anzitutto, che l'interpretazione accolta dalle Sezioni Unite avrebbe portato all'ingresso nei processi italiani di prove che sarebbero da considerare vietate a livello nazionale.

La ragione è che le autorità francesi avrebbero raccolto i messaggi attraverso un'operazione di indiscriminata sorveglianza di massa, mirata non ad acquisire le comunicazioni intercorrenti fra specifiche utenze, ma a carpire senza alcuna limitazione tutti i flussi comunicativi in transito nei *server* di *Sky ECC*[31].

Ciò sarebbe avvenuto tramite un utilizzo del captatore informatico tale da concretizzarsi in una perquisizione occulta non consentita dalle regole italiane[32].

---

[29] In senso favorevole, v. O. CALAVITA, *L'ordine europeo di indagine penale. Presente e futuro della cooperazione probatoria nell'Unione Europea*, Wolters Kluwer-Cedam, 2025, pp. 263 ss.

[30] Sentenza *Gjuzi*, § 9 s.; sentenza *Giorgi*, § 12 s.

[31] Cfr. G.D. CAIAZZA, *Minority Report (svegliatevi, c'è poco da scherzare)*, in *PQM*, 7 dicembre 2024.

[32] Cfr. L. MARAFIOTI, *Chat criptate e tirannie tecnologiche sulla prova*, e O. MAZZA, *Sky-ECC e l'ipocrisia del mutuo riconoscimento*, sempre in *PQM*, 7 dicembre 2024.

Aderendo alle prospettazioni della Procura generale della Corte di cassazione, le Sezioni Unite hanno giustamente replicato come, in realtà, le operazioni francesi potessero considerarsi attività di intercettazione e di sequestro suscettibili di trovare una disciplina nel nostro codice.

È vero che gli artt. 266 commi 2 e 2 *bis*, 267 commi 1 e 2 *bis* e 268 comma 3 c.p.p. configurano il captatore informatico come strumento per svolgere intercettazioni "fra presenti" (ossia ambientali) «su un dispositivo elettronico portatile»: locuzioni che parrebbero escludere le intercettazioni telematiche previste dall'art. 266 *bis* c.p.p., ossia la categoria in cui si sarebbero dovute includere le attività francesi.

Il *modus operandi* di queste ultime, nondimeno, consentiva di ritenerle compatibili con le norme nazionali perlomeno nella sostanza.

Dal punto di vista tecnico, nell'ambito della piattaforma *Sky ECC* i messaggi transitavano attraverso non solo i dispositivi telefonici, ma anche i *server* della compagnia (c.d. architettura *client-server).* Il che significava che non sarebbe stato possibile captarli se non svolgendo le intercettazioni anche all'interno dei *server*.

Il captatore informatico, in questo modo, era stato utilizzato, anche se in modo indiretto, per effettuare intercettazioni su dispositivi portatili, così come previsto dal nostro codice: «l'intercettazione del *server* e l'inoculazione del *trojan*» era stata «servente o strumentale all'intercettazione dei criptofonini», rappresentandone una «naturale e necessaria modalità attuativa»[33].

Il captatore informatico, del resto, integra non un «autonomo mezzo di ricerca della prova», ma «uno strumento tecnico attraverso il quale esperire il mezzo di ricerca della prova costituito dalle intercettazioni di conversazioni o di comunicazioni». Di conseguenza, il riferimento al luogo della sua possibile collocazione non è da considerare tassativo[34].

Mi sembra di poter aggiungere che in un contesto contraddistinto da una grande difficoltà per il legislatore di adeguarsi ai continui sviluppi della tecnologia, aggiornando con sufficiente tempestività il catalogo dei mezzi di ricerca della prova[35], divengono del tutto giustificate le interpretazioni che cercano di riadattare le prescrizioni vigenti alle nuove tecniche investigative; alla condizione, naturalmente, che ne risulti assicurato un adeguato livello di protezione delle garanzie.

Neppure si poteva sostenere che gli atti istruttori delle autorità francesi, diretti ad acquisire i messaggi trasmessi attraverso specifiche utenze telefoniche, sia pure estesi, per forza di cose, ai *server* in cui quei messaggi erano transitati, avessero integrato un'intercettazione "di massa".

---

[33] *Memoria* della Procura generale, p. 62. Lo stesso potrebbe dirsi per le attività ausiliarie che, pur intrusive nei confronti del diritto alla riservatezza, sono indispensabili per svolgere le intercettazioni tradizionali (come la collocazione di microspie all'interno di un luogo di privata dimora): cfr. sentenza *Giorgi*, § 15.4.2.

[34] Cfr. sentenza *Giorgi*, § 15.4.1.

[35] Sull'inadeguatezza delle attuali prescrizioni codicistiche a regolamentare operazioni istruttorie come quelle compiute nel caso *Sky ECC*, v. D. CURTOTTI-V. RIZZI-W. NOCERINO-A. RUSSITTO-G. GILIBERTI-G. SCARPA, *Piattaforme criptate e prova penale*, in questa *Rivista*, fasc. 6, 2023, pp. 194 ss.

Per quanto significativi dal punto di vista quantitativo, essi avevano colpito degli obiettivi predefiniti[36]. Erano stati, inoltre, confinati ad uno spazio - i *server* di *Sky ECC* - non interamente nella disponibilità dei fruitori dei servizi di messaggistica, in rapporto al quale le esigenze di riservatezza erano minori[37].

Il pericolo per la *privacy* che ne era derivato non era stato, peraltro, superiore a quello generato dalle intercettazioni ambientali tramite il captatore a cui si riferisce esplicitamente il nostro codice: le quali permettono di acquisire in modo indiscriminato le conversazioni della persona intercettata a prescindere dal luogo in cui questa venga a trovarsi[38].

La stessa Corte europea dei diritti dell'uomo ha avuto occasione di precisare che le intercettazioni, in linea generale, non potrebbero ritenersi vietate solo a causa della grande entità dei flussi di comunicazioni che esse consentano di captare: un'eventualità sempre più frequente grazie alla tecnologia digitale, che permette la trasmissione di una mole enorme di dati. L'essenziale è che siano soggette a regole e garanzie tali da impedirne l'uso arbitrario[39].

Diverso il discorso se il captatore venisse impiegato per intercettare tutto ciò che avviene all'interno di certi sistemi o reti informatiche senza nessuna predeterminazione di scopo. Si pensi ai *trojan* capaci di acquisire a distanza il contenuto di interi spazi digitali riservati, o di sorvegliarne in modo occulto le attività (ad esempio, captando i dati in entrata e in uscita, gli elenchi dei siti *web* visitati, le immagini visualizzate sullo schermo o le *password* digitate sulla tastiera). Operazioni del genere, a causa della loro totale ed incontrollata pervasività, non possiederebbero i requisiti minimi indispensabili per integrare lo schema normativo di nessuno degli atti di indagine attualmente previsti nel nostro sistema, e neppure potrebbero farsi rientrare nel novero delle prove atipiche *ex* art. 189 c.p.p.[40].

---

[36] Come osserva la *Memoria* della Procura generale, p. 61, la «determinatezza del *target*», in questo caso, era derivata non dal «numero assoluto di utenze», ma dalla «possibilità di distinguere sufficientemente» chi era oggetto delle operazioni «rispetto alla collettività indifferenziata dei fruitori di servizi di comunicazione elettronica».

[37] *Memoria* della Procura generale, p. 47.

[38] In senso analogo, v. la *Memoria* della Procura generale, p. 59: «sarebbe paradossale, del resto, ritenere che la disposizione indicata permetta una intercettazione in astratto più invasiva, perché itinerante, ed impedisca una captazione che lo è certamente di meno perché concentrata in un dispositivo fisso».

[39] Cfr. Corte eur., 25 maggio 2021, *Big Brother Watch ed altri c. Regno Unito*, § 322 s.; Id., 25 maggio 2021, *Centrum för Rättvisa c. Svezia*, § 236 s. G. MILICIA, *Il radioso futuro delle intercettazioni di massa*, in *PQM*, 7 dicembre 2024, obietta che queste pronunce dei giudici di Strasburgo si riferiscono alle intercettazioni c.d. preventive, disposte dai servizi di *intelligence* o di pubblica sicurezza al fine di sorvegliare l'attività di determinati soggetti pericolosi, i cui risultati non sono spendibili nei processi penali. È possibile replicare che esse sono comunque rappresentative dell'attitudine della Corte europea, già emersa in numerose sentenze, a bilanciare la tutela dei diritti fondamentali con le esigenze repressive, specie laddove venga in gioco l'accertamento di gravi reati.

[40] Come tali, dovrebbero ritenersi giuridicamente inesistenti e, quindi, inefficaci: cfr. M. DANIELE, *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Proc. pen. giust.*, f. 5, 2018, pp. 834 s.

7.2. Seconda obiezione*: inidoneità delle norme nazionali sulla circolazione delle prove ad incasellare le operazioni francesi.*

Un'altra obiezione alla lettura offerta dalle Sezioni Unite è quella dell'inidoneità delle norme italiane in tema di circolazione delle prove ad inquadrare le attività istruttorie francesi: le quali, come si è detto, avevano una natura mista, consistendo in intercettazioni tramite captatore informatico a cui erano seguiti dei sequestri.

Si potrebbe infatti sostenere che tale disciplina, pensata in rapporto alle prove acquisite in base alle regole nazionali, non si adatti alle operazioni istruttorie svolte all'estero, poiché non ne discenderebbero condizioni di ammissibilità sufficientemente rigorose.

In riferimento alla circolazione degli atti originariamente non ripetibili - ossia la categoria in cui dovrebbe essere inclusa la raccolta dei messaggi - l'art. 238 comma 3 c.p.p. non pone nessun presupposto di utilizzabilità[41]. Quanto alla circolazione delle intercettazioni, l'art. 270 c.p.p. si limita a richiedere che il procedimento abbia ad oggetto i «delitti per i quali è obbligatorio l'arresto in flagranza" e, qualora si tratti di intercettazioni effettuate con il captatore informatico, i gravi delitti indicati dall'art. 266 comma 2 *bis*.

Si pensi, però, alle conseguenze a cui si andrebbe incontro qualora si concludesse che la circolazione transnazionale di atti istruttori come quelli svolti in Francia, in quanto priva di un equivalente normativo a livello nazionale, non sarebbe consentita. Si tratterebbe di un esito nichilistico, che, tra l'altro, stimolerebbe le organizzazioni criminali italiane ad avvalersi di sistemi informatici di comunicazione situati all'estero, nella consapevolezza che, così operando, i loro messaggi, anche se intercettati, sarebbero processualmente inutilizzabili.

Ecco perché l'approccio delle Sezioni Unite può considerarsi, tutto sommato, condivisibile. La base normativa a sostegno della circolazione dei messaggi ricavabile dagli artt. 78 disp. att., 238 e 270 c.p.p. è senz'altro lacunosa. Ma essa può ritenersi sufficiente nella misura in cui venga integrata dalle garanzie che dovrebbero, in ogni caso, assistere la raccolta transnazionale delle prove tramite l'OEI: le quali, come vedremo, non consentirebbero un uso scriteriato dei messaggi nei procedimenti italiani.

7.3. Terza obiezione*: violazione dell'obbligo di notifica delle intercettazioni alle autorità italiane.*

Una terza obiezione nei confronti dell'impostazione delle Sezioni Unite consiste nel fatto che, stando alla disciplina dell'OEI, le attività svolte dalle autorità francesi, comunque tali da comportare anche delle intercettazioni, avrebbero dovuto essere notificate alle competenti autorità italiane.

[41] I commi 1 e 2 *bis* dell'art. 238 c.p.p., per converso, si riferiscono, rispettivamente, alla circolazione delle «prove assunte nell'incidente probatorio o nel dibattimento» e ai «verbali di dichiarazioni», limitando così il loro raggio operativo alle prove costituende in giudizio.

L'obbligo di notifica, previsto dagli artt. 31 direttiva 41/2014 e 24 d.lgs. 108/2017, concerne le situazioni in cui le intercettazioni, nonostante che abbiano ad oggetto utenze situate all'estero, possono essere svolte senza l'assistenza tecnica dello Stato interessato. La notifica serve, per l'appunto, ad informare quest'ultimo, ponendolo nelle condizioni di vietare l'utilizzo le intercettazioni qualora le stesse fossero proibite in un caso interno analogo. Si mira, in questo modo, ad evitare l'aggiramento delle regole previste da quel sistema[42].

Ebbene, la Corte di giustizia dell'Unione Europea, chiamata ad esprimersi in rapporto al caso *Encrochat*, ha avuto modo di precisare che le operazioni istruttorie come quelle di cui stiamo parlando rientrano senz'altro nella nozione di "intercettazione di telecomunicazioni" disciplinate dall'art. 31 direttiva 41/2014. Tale categoria, al fine di non pregiudicare la cooperazione giudiziaria, va intesa nel senso più ampio, ricomprendendo qualunque forma di «infiltrazione in apparecchiature terminali volta ad estrarre dati di comunicazione, ma anche dati relativi al traffico o all'ubicazione, a partire da un servizio di comunicazione basato su *internet*»[43]. Essa, dunque, include anche le intercettazioni di comunicazioni trasmesse attraverso sistemi o reti informatiche.

Ciò premesso, esiste tuttavia un ulteriore requisito affinché l'obbligo di notifica possa considerarsi esigibile: vale a dire la conoscibilità, da parte dell'autorità che intende eseguire le intercettazioni, del fatto che l'utenza da intercettare si trovi in un determinato Stato straniero.

Ebbene, come pongono in rilievo le Sezioni unite, tale evenienza non ricorreva nel nostro caso[44], laddove, essendo le intercettazioni avvenute anche all'interno dei *server* di *Sky ECC* in cui i messaggi erano transitati, non era stato possibile determinare luoghi specifici in cui i criptofonini erano venuti a collocarsi.

La non circoscrivibilità dal punto di vista geografico, del resto, è una peculiarità che le operazioni istruttorie che avvengono negli spazi digitali possono presentare[45], e che rischia di rendere obsolescente l'obbligo di notifica di cui si discute[46].

Fortunatamente, l'obiettivo della notifica, ossia la possibilità di attivare un vaglio di utilizzabilità delle intercettazioni, può essere perseguito attraverso gli altri *test* di ammissibilità a cui, come ora vedremo, esse non possono sottrarsi.

---

[42] Come rischia di avvenire, ad esempio, con il c.d. instradamento, adottato quando l'intercettazione inizia in un determinato paese, ma deve però proseguire in un altro Stato a causa dei movimenti del titolare dell'utenza. Cfr., riguardo alle rogatorie, Cass., sez. II, 22 luglio 2020, n. 29362.

[43] Corte giust., 30 aprile 2024, *MN*, § 119.

[44] Sentenza *Giorgi*, § 15.5.2. V. anche la *Memoria* della Procura generale, p. 64.

[45] Cfr. S. SIGNORATO, *Le indagini digitali*, cit., pp. 152 ss.

[46] Che la direttiva 41/2014, peraltro, neppure prevede a pena di inutilizzabilità delle intercettazioni effettuate in sua violazione.

8. Tra *lex loci* e *lex fori*: quali garanzie?

Stabilito che i messaggi digitali già raccolti dalle autorità francesi potevano trasmigrare nel nostro sistema sulla base dell'equivalenza con le regole nazionali in tema di circolazione delle prove, viene in gioco il *clou* della vicenda.

La loro acquisizione doveva rispondere a precise condizioni di ammissibilità, tali da assicurare le garanzie che, come si è già detto, dovrebbero assistere la raccolta di qualsiasi prova digitale[47].

Al contempo, le garanzie in questione dovevano essere "riadattate", tenendo conto del fatto che le prove erano state raccolte sulla base di un diritto straniero.

A questo riguardo, le indicazioni impartite dalle Sezioni Unite mi sembrano perlopiù condivisibili, sia pure nei limiti che ora vedremo.

Se ne possono ricavare i seguenti requisiti, che dovrebbero operare ogni volta in cui, come avvenuto nel caso *Sky ECC*, venga in gioco l'acquisizione nei processi italiani tramite l'OEI di prove digitali già in possesso di un'autorità straniera.

8.1. Controllo giurisdizionale duplicato.

Ai fini della circolazione delle prove a livello nazionale, né l'art. 238 né l'art. 270 c.p.p. richiedono l'autorizzazione preventiva di un giudice. Il che consente di affermare che, in applicazione del principio di equivalenza, l'OEI volto alla trasmissione delle prove digitali già raccolte da un'autorità straniera possa essere emesso direttamente da un pubblico ministero.

Su questa conclusione converge anche la decisione della Corte di giustizia sul caso *Encrochat*. Il pubblico ministero, osservano i giudici di Lussemburgo, figura tra i soggetti che, ai sensi dell'art. 2 *c* direttiva 41/2014, possono emettere l'OEI. Di conseguenza, un OEI finalizzato ad ottenere prove già raccolte dalle competenti autorità dello Stato di esecuzione non dovrebbe «essere adottato necessariamente da un giudice quando, in forza del diritto dello Stato di emissione, in un procedimento puramente interno a tale Stato, la raccolta iniziale di tali prove avrebbe dovuto essere ordinata da un giudice, ma competente ad ordinare l'acquisizione di dette prove è il pubblico ministero»[48].

Un approccio del genere si presta ad un'obiezione: come si potrebbe rinunciare al controllo giurisdizionale al fine dello svolgimento di attività istruttorie come le intercettazioni, le quali, nel nostro sistema, richiederebbero l'autorizzazione addirittura preventiva di un giudice[49]?

---

[47] Sulle quali v. *supra*, § 3.

[48] Corte giust., 30 aprile 2024, *MN*, § 69 s.

[49] Cfr. F. GIUNCHEDI, *La natura dei messaggi scambiati via chat ed acquisiti mediante Ordine europeo di indagine e la loro utilizzabilità*, in *Proc. pen. giust.*, f. 1, 2025, pp. 97 ss.

La risposta delle Sezioni Unite è che il controllo giurisdizionale non sparisce del tutto; solo, esso è costretto a sdoppiarsi, a causa delle peculiarità delle operazioni di cui si discute[50].

i) *Autorizzazione* ex ante *di un giudice straniero*. Qualora consista anche in attività di intercettazione, la raccolta delle prove digitali da parte di un'autorità straniera dovrebbe essere, anzitutto, autorizzata *ex ante* da un giudice dello Stato in cui essa sia originariamente avvenuta.

Stando alla ricostruzione operata dalle Sezioni Unite, nel caso *Sky ECC* tale condizione si sarebbe verificata: i messaggi sarebbero stati acquisiti a seguito di provvedimenti autorizzativi emessi da *juges d'instruction* francesi[51], ed «ampiamente motivati» quanto ai presupposti di svolgimento delle operazioni istruttorie[52].

ii) *Controllo* ex post *di un giudice italiano*. Il controllo da parte del solo giudice straniero non sarebbe sufficiente: dal sistema dell'OEI emerge chiaramente come sia indispensabile un vaglio, perlomeno successivo, operato anche da un giudice dello Stato di emissione.

Lo si ricava, in primo luogo, dall'art. 14 § 1 e 2 direttiva 41/2014, ai sensi del quale agli atti istruttori richiesti nell'OEI dovrebbero essere applicabili «mezzi d'impugnazione equivalenti a quelli disponibili in un caso interno analogo».

Ma se ci si limitasse al solo principio di equivalenza, la tutela rischierebbe di essere insufficiente: nessun controllo opererebbe qualora la legislazione nazionale dello Stato di emissione dell'OEI non prevedesse un mezzo di impugnazione a livello domestico.

Questa è la ragione per cui la Corte di giustizia ha ritenuto di alzare l'asticella con la ben nota sentenza *Gavanozov II*[53], introducendo uno *standard* di tutela indipendente dalle caratteristiche degli ordinamenti dei singoli Stati. Un controllo giurisdizionale da parte dello Stato di emissione – hanno chiarito i giudici di Lussemburgo – dovrebbe essere assicurato perfino quando tale garanzia non fosse contemplata in rapporto ad un caso interno analogo[54].

Ebbene, in riferimento al caso *Sky ECC*, le Sezioni Unite hanno affermato che, al fine di assicurare tale controllo giurisdizionale, sarebbe stato sufficiente il vaglio operato

---

[50] Più in generale, sulle varie modulazioni che può assumere il controllo giurisdizionale nell'ambito della raccolta transnazionale delle prove tramite l'OEI v. A. MOSNA, *Judicial protection in EU cross-border Evidence-Gathering: the EIO as a Case Study*, in *Eur. Crim. Law Rev.*, f. 2, 2024, pp. 171 ss.

[51] Organi che, per quanto dotati anche di poteri investigativi, in quel sistema sono indipendenti dal governo, e possono quindi essere considerati veri e propri giudici.

[52] Sentenza *Giorgi*, § 18.5.1; sentenza *Gjuzi*, § 12.4. Nello stesso senso la *Memoria* della Procura generale, p. 27: «trattasi di provvedimento emesso dall'autorità giudiziaria francese, con ampia e specifica motivazione e secondo *standard* addirittura superiori a quelli previsti nell'ordinamento nazionale italiano: infatti, nella motivazione – ben oltre i requisiti minimi di cui all'art. 267 c.p.p. – è argomentata l'indispensabilità del mezzo».

[53] Relativa all'emissione di un OEI da parte della Bulgaria ai fini dello svolgimento di perquisizioni, sequestri e audizioni in videoconferenza, atti nei cui confronti il diritto bulgaro non prevedeva un controllo giurisdizionale a livello nazionale.

[54] Pur non contemplato dalla direttiva 41/2014, tale obbligo è stato ricavato dai giudici di Lussemburgo dal diritto ad un ricorso effettivo previsto dall'art. 47 della Carta dei diritti fondamentali dell'Unione Europea (c.d. Carta di Nizza): cfr. Corte giust., 11 novembre 2021, C-852/19, *Gavanozov II*, § 24 s.

dal giudice nazionale chiamato ad utilizzare le prove, dotato del potere di valutare se vi fossero i presupposti per «ammetterle»[55].

C'è da chiedersi se una conclusione del genere sia compatibile con quanto affermato dalla sentenza *Gavanozov II*, la quale, in taluni suoi passaggi, richiede testualmente la previsione di un "mezzo d'impugnazione" ("*legal remedy*") contro l'emissione di un ordine europeo di indagine[56].

La risposta è da ritenere affermativa, se si tiene conto che quella sentenza non è sempre così netta nell'identificare il contenuto del controllo giurisdizionale nei confronti dell'emissione di un OEI. Basti pensare che la Corte di giustizia, ad un certo punto, afferma che il contenuto del diritto ad un ricorso effettivo *ex* art. 47 Carta di Nizza «corrisponde» a quello dell'omologo diritto statuito dall'art. 13 CEDU, così come esso viene inteso dalla Corte europea dei diritti dell'uomo[57].

A sua volta, la Corte europea parla, più genericamente, di «accesso» a un procedimento» che «consenta» di «contestare la regolarità e la necessità» dei mezzi istruttori, e di «ottenere un adeguato rimedio qualora tali misure siano state disposte o eseguite illegalmente»[58]: il che non richiede necessariamente la previsione di uno specifico mezzo di impugnazione, se si pensa che tale opportunità di contestazione potrebbe essere assicurata anche solo di fronte al giudice deputato ad utilizzare quelle prove.

Vi sono buone ragioni, insomma, per ritenere che il controllo giurisdizionale sdoppiato, così come configurato dalle Sezioni Unite, assicuri gli *standard* di garanzia richiesti dalla direttiva 41/2014 e dalla Corte di giustizia dell'Unione Europea.

8.2. Vaglio di proporzionalità ripartito.

Alla duplicazione del controllo giurisdizionale corrisponde una suddivisione di compiti in merito al vaglio di proporzionalità.

È di competenza del giudice straniero verificare *ex ante* la presenza dei presupposti per lo svolgimento delle operazioni istruttorie previsti dal proprio diritto: la giustificazione fattuale, la stretta necessità e l'attinenza del procedimento a reati di una certa gravità.

Al giudice italiano deputato ad utilizzare le prove digitali raccolte all'estero anche tramite attività di intercettazione, dal canto suo, senz'altro spetta un controllo *ex post* sulla circostanza che il procedimento riguardi uno dei reati elencati dall'art. 270 c.p.p.: un requisito che, nel caso *Sky ECC*, poteva dirsi rispettato, considerato che le indagini avevano ad oggetto il grave delitto di associazione per delinquere finalizzata al traffico di stupefacenti[59].

---

[55] Sentenza *Gjuzi*, § 9.4 s.; sentenza *Giorgi*, § 12.4 s. Nello stesso senso, si veda la *Memoria* della Procura Generale, pp. 35 s.

[56] Corte giust., 11 novembre 2021, *Gavanozov II*, § 33.

[57] Corte giust., 11 novembre 2021, *Gavanozov II*, § 34.

[58] Cfr., ad esempio, Corte eur., 19 gennaio 2017, *Posevini c. Bulgaria*, § 84 s.

[59] Sentenza *Giorgi*, § 18.5.4.

Ciò premesso, il giudice italiano dovrebbe svolgere anche tutti gli altri controlli previsti dalla legge nazionale nei casi interni analoghi?

Qui viene in gioco un problema cruciale della raccolta transnazionale delle prove, legato alla diversità dei diritti probatori degli Stati volta per volta interessati. La risposta affermativa al quesito, idealmente parlando, sarebbe la più corretta. In concreto, però, creerebbe non pochi inconvenienti. L'autorità straniera dovrebbe trasmettere all'autorità italiano il fascicolo completo del procedimento, tradotto in italiano o in una lingua veicolare. La necessità di osservare tutte le condizioni previste non solo dalla *lex loci*, ma anche dalla *lex fori*, inoltre, potrebbe mettere in dubbio la spendibilità delle prove nei processi nazionali.

Questa è la ragione per cui la cooperazione giudiziaria si ispira all'ideale del mutuo riconoscimento, che rappresenta una soluzione obbligata in un contesto in cui i vari diritti probatori nazionali mantengono non poche inconciliabilità.

Lo mette in rilievo la Corte di giustizia UE in riferimento al caso *Encrochat*, laddove osserva che l'autorità di emissione dell'OEI, quando intenda ottenere la trasmissione di prove già in possesso delle competenti autorità dello Stato di esecuzione, «non» potrebbe «controllare la regolarità del distinto procedimento con il quale lo Stato membro di esecuzione ha raccolto le prove di cui essa chiede la trasmissione». Diversamente, si correrebbe il rischio rendere il «sistema più complesso e meno efficace», in violazione della fiducia reciproca che dovrebbe contraddistinguere i rapporti fra gli Stati dell'Unione Europea[60].

Al contempo, con una forte dose di equivocità, sia nella direttiva 41/2014 sia, più in generale, negli stessi trattati dell'Unione Europea, si legge che il mutuo riconoscimento non deve essere attuato in modo integralistico, ma va contemperato con la tutela dei diritti fondamentali; e quindi – verrebbe da dire – anche con il modo in cui questi ultimi vengono protetti dalla legislazione dello Stato in cui le prove raccolte all'estero dovrebbero essere utilizzate[61].

La stessa ambiguità emerge dalla decisione *Encrochat* della Corte di giustizia[62], nella parte in cui afferma che «il carattere necessario e proporzionato» dell'emissione dell'OEI dovrebbe essere valutato anche alla luce del diritto dello Stato di emissione[63], evitando di aggirarlo[64]. Di conseguenza, se l'acquisizione delle prove dovesse «o apparire sproporzionata ai fini dei procedimenti penali avviati a carico dell'interessato nello Stato di emissione, ad esempio in ragione della gravità della violazione dei diritti fondamentali di quest'ultimo, oppure essere stata disposta in violazione del regime giuridico applicabile a un caso interno analogo, l'organo giurisdizionale investito del

[60] Si veda Corte giust., 30 aprile 2024, *MN*, § 99 e 100. Similmente, cfr. S. RAGAZZI-F. SPIEZIA, *Decifrare, acquisire e utilizzare le comunicazioni criptate in uso alla criminalità organizzata: uno sguardo europeo, in attesa del count-down italiano*, in questa *Rivista*, fasc. 2, 2024, pp. 223 ss.

[61] Basti pensare alle clausole di protezione dei diritti fondamentali previste, in particolare, dall'art. 1 § direttiva 41/2014 e dall'art. 6 TUE.

[62] Cfr. L. BERNARDINI, *On Encrypted Messages and Clear Verdicts - the EncroChat Case before the Court of Justice (Case C-670/22, MN)*, in *eulawlive.com*, 21 maggio 2024.

[63] Si veda Corte giust., 30 aprile 2024, *MN*, § 88 e 89.

[64] Cfr. Corte giust., 30 aprile 2024, *MN*, § 97 e 98.

ricorso contro l'ordine europeo di indagine che dispone tale trasmissione dovrebbe trarne le conseguenze che si impongono in base al diritto nazionale»[65].

Non è facile ricavarne indicazioni precise per i giudici dello Stato di emissione, schiacciati fra l'esigenza di fidarsi dell'operato delle autorità straniere, in modo da non pregiudicare la cooperazione giudiziaria, e la necessità di proteggere i diritti fondamentali anche sulla base delle regole del proprio diritto.

Un punto di equilibrio può essere trovato cercando di fissare degli *standard* minimali di protezione dei diritti al di sotto dei quali non sarebbe possibile scendere. In questa direzione, un contributo decisivo è offerto dalle decisioni con cui la Corte di giustizia e la Corte europea dei diritti dell'uomo mirano ad armonizzare i vari diritti nazionali, individuando delle garanzie comuni[66].

Se ne può ricavare, in particolare, che il diritto alla riservatezza *ex* artt. 8 CEDU e 7 Carta di Nizza potrebbe essere compresso per fini investigativi solo in presenza di una solida giustificazione, tale da dimostrare che esso non sia stato violato in modo arbitrario[67].

Ciò consente di affermare che il giudice italiano competente a stabilire se le prove raccolte con l'OEI siano utilizzabili nei processi nazionali dovrebbe svolgere un controllo, per l'appunto, sulla motivazione dei provvedimenti istruttori adottati dalle autorità straniere.

In applicazione della logica del mutuo riconoscimento, tale vaglio non potrebbe spingersi fino ad un raffronto fra la motivazione e gli atti del procedimento. Tuttavia, il giudice italiano dovrebbe perlomeno avere la possibilità di individuare eventuali illogicità, nella misura in cui queste emergessero dal testo della motivazione.

Ebbene, mi sembra che nel caso *Sky ECC* le Sezioni Unite abbiano svolto proprio un controllo di questo tipo, ponendo in evidenza come la giustificazione addotta dal giudice istruttore francese a sostegno della raccolta dei messaggi fosse, in sé considerata, sufficientemente robusta[68].

---

[65] Corte giust., 30 aprile 2024, *MN*, § 102 e 103.

[66] Cfr. R.E. KOSTORIS, *La tutela dei diritti fondamentali*, in ID. (a cura di), *Manuale di procedura penale europea*, V ed., Giuffrè, 2022, pp. 113 ss.

[67] V., fra le molte, Corte eur., 20 novembre 2018, *Erduran and Em Export Diş Tic. A.s. c. Turchia*, § 79 s.; Id., 10 marzo 2009, *Bykov c. Russia*, § 76 s. Analogamente, Corte giust., 4 ottobre 2024, *CG*, § 84 s.

[68] Sentenza *Giorgi*, § 18.5.1 s., in cui si legge che l'attività di intercettazione e di sequestro era giustificata da vari elementi, quali: l'uso da parte degli utenti di un economicamente dispendioso sistema informatico di trasmissione di messaggi secretati, tale da garantire l'anonimato; il fatto che quel sistema, in altri casi, fosse stato usato da organizzazioni criminali transnazionali; l'impiego di un metodo di crittografia altamente sofisticato. L'uso di captatori informatici, dal canto suo, era «l'unico mezzo per decifrare i messaggi individuali degli utilizzatori del sistema di crittografia in questione, determinare il livello di utilizzazione criminale dello stesso, identificare i dirigenti della società *Sky Global* che lo gestiva e conoscere i legami di costoro con le organizzazioni criminali».

8.3. Obbligo di adottare le migliori tecniche informatiche secondo il diritto straniero.

Le modalità di svolgimento delle indagini informatiche, nel caso delle prove digitali già autonomamente raccolte all'estero, non potrebbero che essere regolate dal diritto straniero.

Nondimeno, le conseguenze della violazione dell'obbligo di impiegare le migliori tecniche informatiche, previsto, come si è visto, nel nostro sistema[69], dovrebbero essere valutate dal punto di vista delle norme italiane.

A tale riguardo, vedremo come in ipotesi del genere l'esito non sarebbe l'inutilizzabilità delle prove raccolte all'estero, ma una diminuzione del loro valore conoscitivo, di cui il giudice dovrebbe dare conto nella motivazione della decisione[70].

8.4. Contraddittorio tecnico posticipato secondo il diritto italiano.

Qualora, come nel caso *Sky ECC*, l'acquisizione delle prove digitali avvenga all'estero attraverso operazioni occulte di intercettazione, è evidente che non sarebbe possibile applicare un contraddittorio di tipo contestuale.

Dovrebbe, però, essere perlomeno assicurato un contraddittorio di tipo posticipato nel contesto del procedimento italiano: vale a dire, come si è già detto, la possibilità per le parti di interloquire, anche con l'ausilio di esperti, sulle modalità di raccolta delle prove.

La sua importanza è testimoniata dal fatto che tale forma di contraddittorio può essere fatta rientrare in un più generale diritto che emerge in varie sentenze della Corte di giustizia, da ultimo ribadito in relazione al caso *Encrochat*. Alludo all'opportunità per le parti di «svolgere efficacemente le proprie osservazioni» in merito alle prove raccolte: un requisito che, come vedremo, è addirittura considerato dai giudici di Lussemburgo come condizione di utilizzabilità delle prove[71].

8.5. Catena di custodia secondo il diritto straniero.

Per assicurare il contraddittorio tecnico, l'autorità straniera dovrebbe preservare la catena di custodia in base al proprio diritto, trasmettendo alle autorità italiane una documentazione idonea a rappresentare l'intero ciclo di raccolta dei messaggi.

Lo si può ricavare, più in generale, dall'obbligo di trasparenza fra gli Stati che dovrebbe contraddistinguere la raccolta delle prove tramite gli strumenti di cooperazione giudiziaria: il quale, purtroppo, spesso viene dimenticato arroccandosi dietro il paravento della fiducia reciproca[72].

---

[69] Si veda la tebella riportata nel § 3.

[70] *Infra*, § 8.6 s.

[71] *Infra*, § 8.6.

[72] Cfr. M. PANZAVOLTA, *Formal and Informal Circulation of Cross-Border Evidence in Europe and Possible Improvements: Toward an "Annex E" of the European Investigation Order?*, in *Eur. Crim. Law Rev.*, f. 2, 2024, pp.

Proprio a questo proposito, vedremo come nel caso *Sky ECC* si sia registrato un vuoto di tutela legato alle peculiarità delle tecniche informatiche con cui i messaggi erano stati acquisiti[73].

8.6. Inutilizzabilità rilevabili dal giudice italiano.

Una domanda cruciale, come è agevole comprendere, è se l'inosservanza dei requisiti di acquisizione delle prove digitali fin qui considerati genererebbe dei divieti probatori.

Salva un'eccezione[74], divieti del genere non figurano in modo espresso nella direttiva 41/2014, a testimonianza dell'incapacità degli Stati dell'Unione Europea di accordarsi sulla previsione di regole comuni di utilizzabilità delle prove: un difetto che da sempre contraddistingue la cooperazione giudiziaria, e che l'introduzione dell'OEI non è riuscita a superare.

Ciò non significa, tuttavia, che sia impossibile ricavare indicazioni più nette dal sistema dell'OEI considerato nel suo complesso. Per quanto la Corte di giustizia sia solita ripetere che le questioni di ammissibilità delle prove sono principalmente di competenza degli Stati nazionali[75], non si potrebbe sostenere che il diritto UE sia del tutto indifferente al problema[76].

Tanto è vero che gli stessi giudici di Lussemburgo, in due decisioni relative alla materia della conservazione dei dati personali, hanno anzitutto individuato una fonte di inutilizzabilità delle prove nel più sopra considerato principio di equivalenza[77]. «In assenza di norme dell'UE in materia» – ha osservato la Corte di giustizia – «le norme procedurali per le azioni volte a salvaguardare i diritti che gli individui traggono dal diritto dell'UE» dovrebbero essere «non meno favorevoli delle norme che disciplinano azioni analoghe a livello nazionale»[78]. Se ne può ricavare che, se a livello nazionale una certa prova sarebbe esclusa nel processo, la stessa sorte dovrebbe in linea di massima toccare alle prove raccolte all'estero con l'OEI in un caso analogo.

Il principio di equivalenza, da solo, rischia però di essere insufficiente, nella misura in cui la legge dello Stato di emissione dell'OEI non preveda adeguati divieti

206 ss., in cui si suggerisce, *de iure condendo*, l'introduzione nella disciplina dell'OEI di un apposito allegato finalizzato ad incrementare l'apporto informativo che l'autorità di esecuzione dovrebbe assicurare a favore dell'autorità di emissione.

[73] *Infra*, § 9 s.

[74] Mi riferisco all'art. 31 § 3 *b* della direttiva, ai sensi del quale l'autorità competente dello Stato che abbia ricevuto una notifica in merito allo svolgimento di intercettazioni sul suo territorio (*supra*, § 7.3) può disporne l'inutilizzabilità dei risultati quando esse non sarebbero ammesse in un caso interno analogo.

[75] Cfr. ad esempio Corte giust., 6 ottobre 2020, C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e altri*, § 222 s.

[76] Si vedano M. PANZAVOLTA-E. MAES, *Exclusion of evidence in times of mass surveillance. In search of a principled approach to exclusion of illegally obtained evidence in criminal cases in the European Union*, in *Int. Journ. Evidence and Proof*, f. 26, 2022, pp. 202 ss.

[77] V. *supra*, § 7.

[78] Corte giust., 6 ottobre 2020, *La Quadrature du Net*, § 222 s., e Id., 2 marzo 2021, C-746/18, *Prokuratuur*, C-746/18, § 41 s., in merito alla questione della conservazione dei dati di traffico.

probatori. La Corte di giustizia pare esserne consapevole, nella misura in cui ha aggiunto che si deve altresì tenere conto dell'esigenza di evitare che le norme procedurali nazionali «rendano impossibile nella pratica o eccessivamente difficile l'esercizio dei diritti conferiti dal diritto dell'UE» (c.d. principio di effettività)[79].

Nè i giudici di Lussemburgo trascurano il principio di proporzionalità, che va osservato, oltrechè a livello nazionale, anche nel contesto della cooperazione giudiziaria, ed è suscettibile di produrre i suoi effetti pure sul terreno dell'utilizzabilità delle prove raccolte tramite l'OEI[80].

La Corte di giustizia, peraltro, puntualizza come quella dell'inutilizzabilità delle prove non sia una strada obbligata. L'effettività e la proporzionalità potrebbero essere raggiunte anche «mediante norme e prassi nazionali che disciplinano la valutazione e la ponderazione di tale materiale, o tenendo conto dell'eventuale illiceità di tale materiale nella determinazione della pena»[81].

È possibile, nondimeno, ricavare un argomento a favore della presenza di veri e propri divieti probatori nell'art. 14 § 7 direttiva 41/2014. È vero che quest'ultimo si limita a richiedere il rispetto dei «diritti della difesa» e delle «garanzie del giusto processo nel *valutare* le prove acquisite tramite l'OEI». Ma nulla vieta di leggere l'espressione "valutazione" alla luce, per l'appunto, dei principi di effettività e di proporzionalità, intendendola come "valutazione dell'ammissibilità" delle prove[82].

Di qui l'obbligo per il giudice nazionale di dichiarare inammissibili le prove raccolte in violazione del diritto di difesa e dell'equità del procedimento. Una conclusione non molto diversa è, del resto, raggiunta a livello nazionale pure dall'art. 36 d.lgs. 108/2017: il quale prescrive che sono utilizzabili i «verbali degli atti» «assunti all'estero a seguito di ordine di indagine ai quali i *difensori* sono stati posti in grado di assistere e di esercitare le *facoltà* loro consentite dalla legge italiana»[83], rinviando così anch'esso al generale parametro del diritto di difesa.

Mi sembra che proprio questo, nel caso *Sky ECC*, sia stato il modo di ragionare delle Sezioni Unite, le quali, come si è detto, hanno conferito al giudice italiano un controllo di utilizzabilità dei messaggi digitali raccolti in Francia[84]. Come recita uno dei principi di diritto enunciati dalla Corte di cassazione, «l'*utilizzabilità* del contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, e trasmessa sulla base di ordine europeo di indagine, deve essere *esclusa* se il giudice italiano rileva che il loro impiego determinerebbe una *violazione* dei *diritti fondamentali*»[85].

---

[79] Si veda Corte giust., 6 ottobre 2020, *La Quadrature du Net*, § 223, 225.

[80] Cfr. Corte giust., 30 aprile 2024, *MN*, § 103.

[81] Corte giust., 6 ottobre 2020, *La Quadrature du Net*, § 225.

[82] V. anche, in questo senso, M. DANIELE, *Scope of Judicial Review in the Executing State in EIO Proceedings*, in *Eur. Crim. Law Rev.*, f. 2, 2024, pp. 187 s.

[83] Si tratta della medesima regola prevista dall'art. 431 comma 1 lett. *d* c.p.p. per l'utilizzabilità delle prove raccolte tramite le rogatorie.

[84] Sentenza *Gjuzi*, § 9.4 s.; sentenza *Giorgi*, § 12.4 s. In dottrina, cfr. E. LORENZETTO, *L'acquisizione all'estero di comunicazioni digitali criptate nella fucina dell'ordine europeo di indagine penale*, in *Cass. pen.*, 2024, pp. 2896 ss.

[85] Sentenza *Gjuzi*, § 13; sentenza *Giorgi*, § 16.

Certo, un'affermazione del genere apre non poche incertezze. Un'inutilizzabilità fondata sulla violazione di "diritti" individuati in modo generico non è, evidentemente, costruita come una fattispecie capace di delineare in modo esaustivo i propri requisiti operativi, come avviene per i divieti probatori previsti a livello interno. Esattamente quali, tra le innumerevoli regole probatorie nazionali, potrebbero ritenersi poste a tutela del diritto di difesa e delle garanzie del giusto processo o, comunque, di diritti fondamentali, e sarebbero, quindi, da considerare rilevanti ai fini dell'inutilizzabilità?

Le Sezioni Unite osservano che tali regole non andrebbero identificate con «tutte le disposizioni previste dall'ordinamento giuridico italiano in tema di formazione ed acquisizione» delle prove trasmesse con l'OEI, considerato che nessuna norma della direttiva e del d.lgs. 108/2017 prevede, «ai fini dell'utilizzabilità degli atti formati all'estero, la necessità di una puntuale applicazione di tutte le regole che l'ordinamento giuridico italiano fissa, in via ordinaria, per la formazione degli atti corrispondenti formati sul territorio nazionale»[86]. Ma si tratta, evidentemente, di una precisazione insoddisfacente.

8.6.1. Quattro divieti probatori.

Al fine di evitare che un'inutilizzabilità così costruita dia luogo a valutazioni eccessivamente discrezionali, determinando incertezze applicative e disparità di trattamento, è necessario ancorarne la portata alle indicazioni dei diritti nazionali degli Stati coinvolti nella raccolta della prova, nonché del diritto UE e della CEDU.

Ciò comporta che, in riferimento alle operazioni istruttorie come quelle avvenute nel caso *Sky ECC*, il suo contenuto vada definito sulla base delle garanzie fin qui considerate, la cui inosservanza determinerebbe violazioni del diritto di difesa e dell'equo processo tali da risultare inaccettabili in qualsiasi Stato dell'Unione Europea.

Se ne possono ricavare, anzitutto, le seguenti ipotesi:

i) *inutilizzabilità qualora la raccolta delle prove non fosse stata* ab origine *autorizzata da un giudice straniero*

ii) *inutilizzabilità qualora le prove fossero stati acquisite nell'ambito di procedimenti non attinenti ad uno dei gravi reati elencati dall'art. 270 c.p.p.*

iii) *inutilizzabilità qualora la raccolta all'estero delle prove fosse avvenuta sulla base di un provvedimento autorizzativo privo di una motivazione dotata di logicità intrinseca*

Si può aggiungere un ulteriore requisito di utilizzabilità, elaborato dalla Corte di giustizia a partire dalle più sopra menzionate decisioni relative alla protezione dei dati

[86] Sentenza *Gjuzi*, § 7.5 s.; sentenza *Giorgi*, § 10.5 s. Nello stesso senso, rispetto alle rogatorie, v. Cass., sez. un., 25 febbraio 2010, n. 15208, *Mills*.

personali, e poi ripreso dalla decisione *Encrochat* sulla base dell'art. 14 § 7 direttiva 41/2014[87].

Nelle parole dei giudici di Lussemburgo, la «necessità di escludere informazioni ed elementi di prova ottenuti in violazione delle prescrizioni del diritto dell'Unione deve essere valutata alla luce, in particolare, del rischio che l'ammissibilità di tali informazioni ed elementi di prova comporta per il rispetto del principio del contraddittorio e, pertanto, del diritto a un processo equo». Di conseguenza, «un giudice che ritenga che una parte non sia in grado di svolgere in modo efficace le proprie osservazioni in merito a un mezzo di prova»[88] che possa «influenzare in modo preponderante la valutazione dei fatti» dovrebbe «constatare una violazione del diritto a un processo equo ed *escludere* tale mezzo di prova al fine di evitare una violazione del genere»[89].

Ecco, quindi, un quarto divieto probatorio:

iv) *inutilizzabilità qualora le parti non siano poste in grado di svolgere con efficacia le proprie osservazioni in merito all'acquisizione e al valore delle prove*

Quest'ultima regola di esclusione mira, evidentemente, a proteggere il diritto ad un contraddittorio tecnico perlomeno di tipo posticipato.

Ne deriva, altresì, uno stimolo ad adottare un'adeguata catena di custodia, così da permettere di ricostruire in modo puntuale come le prove sono state effettivamente raccolte.

Mi sembra, invece, che non sia consentito individuare un'inutilizzabilità legata al mancato impiego delle migliori tecniche informatiche al fine dell'acquisizione delle prove digitali.

Un divieto probatorio del genere mirerebbe principalmente a proteggere l'attendibilità dell'accertamento; non verrebbe, quindi, necessariamente in gioco il rischio di una lesione del diritto di difesa o dei principi del giusto processo.

Del resto, sebbene non sia un assunto unanimemente condiviso, si può ritenere che tale divieto non sarebbe ravvisabile neppure in relazione ad un caso nazionale analogo[90]. La ragione è comprensibile: si tratterebbe di un'inutilizzabilità inscindibilmente legata alle opinioni degli esperti chiamati a valutare la validità delle tecniche impiegate; ma queste ultime potrebbero anche originare dubbi o contrasti, rendendone incerta l'operatività.

---

[87] V. A. MOSNA, *Judicial protection*, cit., p. 174.

[88] Tale diritto è formulato in termini analoghi anche dalla Corte europea dei diritti dell'uomo, secondo la quale l'accusato dovrebbe avere l'opportunità di accedere alle prove e di analizzarle: cfr. Corte eur., 26 settembre 2023, *Yüksel Yalçinkaya c. Turchia*, § 306 s.; Id., 4 giugno 2019, *Rook c. Germania*, § 56 s.

[89] Corte giust., 6 ottobre 2020, *La Quadrature du Net*, § 226 s.; v. anche Id., 2 marzo 2021, *Prokuratuur*, § 44; Id., 30 aprile 2024, *MN*, § 104 s. e 130 s.

[90] Cfr. M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, pp. 293 s. Analogamente, in giurisprudenza, Cass., sez. III, 8 giugno 2021, n. 32653. In senso contrario, cfr. L. MARAFIOTI, *Digital evidence e processo penale*, in *Cass. pen.*, 2011, pp. 4521 ss.,

8.6.2. L'onere della prova dell'inutilizzabilità.

Così ricostruito l'ambito operativo dell'inutilizzabilità, altra questione è a chi spetti provarne i requisiti operativi.

A questo riguardo, viene senz'altro in gioco la regola generale secondo cui spetta a chi afferma l'esistenza di un'invalidità processuale addurre i fatti che ne sono a fondamento[91]. Nel contesto della raccolta transazionale delle prove tramite l'OEI, poi, in applicazione della logica della fiducia reciproca che discende dal principio del mutuo riconoscimento, si può dire che viga una "presunzione relativa" di conformità ai diritti fondamentali delle attività istruttorie svolte dalle autorità giudiziarie degli Stati dell'Unione[92].

Ciò ha permesso alle Sezioni Unite di precisare che «l'onere di allegare e provare i fatti da cui inferire la violazione di diritti fondamentali» graverebbe «sulla difesa, quando è questa a dedurre l'inutilizzabilità o l'invalidità di atti istruttori acquisiti dall'autorità giudiziaria italiana mediante OEI»[93].

Mi pare che sia un onere esigibile in merito alle inutilizzabilità legate all'assenza di un controllo da parte del giudice straniero o all'attinenza del procedimento a reati diversi da quelli individuati dalla legge per lo svolgimento degli atti istruttori (*sub i* e *ii*), oppure all'assenza di un provvedimento autorizzativo debitamente motivato (*sub iii*): circostanze che, in linea di principio, la difesa può essere in grado di allegare.

Diverso il discorso per il divieto probatorio connesso all'impossibilità per le parti di svolgere con efficacia le proprie osservazioni in merito all'acquisizione e al valore delle prove (*sub iv*). Qui un'applicazione automatica ed indifferenziata dell'onere della prova indicato dalle Sezioni unite potrebbe risultare irragionevole. Non andrebbe, infatti, trascurata la possibile incapacità della difesa di venire a conoscenza in modo sufficientemente preciso delle modalità di svolgimento delle attività istruttorie: una variabile che, quando si ha a che fare con la raccolta di prove digitali, possiede un suo peso specifico.

Alludo ad un problema che prescinde dal carattere transnazionale delle operazioni istruttorie, ponendosi anche a livello interno, e che dipende dalla mancanza di trasparenza che, come vedremo, può talvolta contraddistinguere le indagini informatiche.

Non è da escludere, pertanto, che la parte interessata non sia nelle condizioni di dimostrare l'esistenza della lesione di un diritto fondamentale a causa di un'incolpevole ignoranza di quanto accaduto nel corso delle attività di acquisizione delle prove. E il giudice italiano chiamato a vagliare l'utilizzabilità delle prove non potrebbe non tenerne conto[94].

---

[91] È affermazione ricorrente in giurisprudenza che l'onere di provare il fatto processuale da cui dipenda l'accoglimento di un'eccezione gravi sulla parte che abbia sollevato quest'ultima: v. ad esempio Cass., sez. III, 26 gennaio 2024, n. 12225.

[92] *Considerando* 19 della direttiva. V. anche Corte giust., *Gavanozov II*, § 54.

[93] Sentenza *Gjuzi*, § 7.6; sentenza *Giorgi*, § 10.6.

[94] *Infra*, § 9 s.

8.7. Valutazione motivata secondo il diritto italiano.

La valutazione delle prove digitali già raccolte all'estero e trasmesse con l'OEI dovrebbe, infine, avvenire secondo le regole nazionali (artt. 192 e 546 c.p.p.).

Trattandosi di prove acquisite sulla base di norme straniere magari diverse dalle nostre, il giudice, nello stabilirne il peso conoscitivo, non potrebbe fare a meno di considerare anche le concrete modalità istruttorie della loro acquisizione. L'eventuale impiego di tecniche informatiche scorrette, in particolare, avrebbe come esito quello di screditarne il valore. In tali evenienze, per non rischiare di incorrere in un vizio di motivazione, il giudice dovrebbe andare alla ricerca nel restante materiale probatorio di elementi di riscontro sufficientemente solidi da compensarne i *deficit* cognitivi.

8.8. Tabella di sintesi.

Le garanzie individuate nei paragrafi precedenti possono essere così rappresentate.

GARANZIE OEI	**Autorizzazione da parte di un giudice (controllo giurisdizionale preventivo)**	**Impugnazione (controllo giurisdizionale successivo)**	**Proporzionalità**	**Uso delle migliori tecniche informatiche**	**Contraddittorio tecnico posticipato**	**Catena di custodia**	**Inutilizzabilità (controllo giurisdizionale successivo)**	**Valutazione motivata**
Acquisizione tramite l'OEI delle prove digitali già in possesso dell'autorità giudiziaria straniera: EQUIVALENZA con la disciplina nazionale della circolazione delle prove (art. 6 § 1 *b* direttiva OEI; art. 27 co. 1 d.lgs. 108/2017; art. 78 disp. att. c.p.p.; artt. 238 e 270 c.p.p.)	**giudice straniero**, laddove in un caso interno analogo fosse richiesto un controllo giurisdizionale preventivo		presupposti per lo svolgimento delle operazioni istruttorie previsti dal **diritto straniero** **diritto italiano** (art. 7 d.lgs. 108/2017): - attinenza del procedimento ai reati elencati dall'art. 270 c.p.p. - logicità intrinseca della motivazione del provvedimento straniero	**diritto straniero**	**diritto italiano** (artt. 220 s., 501, 523 c.p.p.)	**diritto straniero**, con trasmissione della documentazione all'autorità italiana	**giudice italiano** (art. 14 § 1 direttiva OEI, Corte di giustizia *Gavanozov II*) **divieti probatori** (art. 14 § 7 direttiva OEI, art. 36 d.lgs. 108/2017): - omessa autorizzazione da parte del giudice straniero - non attinenza del procedimento ai reati elencati dall'art. 270 c.p.p. - motivazione del provvedimento straniero affetta da illogicità intrinseca - impossibilità per le parti di svolgere osservazioni in merito all'acquisizione e al valore delle prove (Corte giust. *MN Encrochat*)	**diritto italiano** (artt. 192, 546, 533 c.p.p.)

9. L'omessa *discovery* degli algoritmi di decriptazione.

Ricostruite le garanzie da osservare ai fini dell'acquisizione tramite l'OEI dei messaggi digitali già autonomamente raccolti all'estero, è necessario considerare il profilo forse più delicato del caso *Sky ECC.*

I messaggi, come si è detto, erano stati scambiati in forma criptata, al fine di salvaguardarne la riservatezza. Per renderli intellegibili, le autorità francesi si erano avvalse di chiavi di decriptazione che non erano state comunicate alle autorità italiane, restando così inaccessibili per la difesa e per i giudici dei procedimenti nazionali.

Ci si imbatte, qui, in un'evenienza frequente quando si ha a che fare con le indagini informatiche, suscettibile di verificarsi anche a livello nazionale. Basti pensare alle intercettazioni tramite il captatore svolte ai sensi degli artt. 266 ss. c.p.p., le quali pure possono essere contraddistinte da un'incompleta *discovery* delle relative modalità di svolgimento.

A quest'ultimo riguardo, la seconda frase dell'art. 89 comma 1 disp. att. c.p.p. prescrive che il verbale delle operazioni dovrebbe indicare «il tipo di programma impiegato e, ove possibile, i luoghi in cui si svolgono le comunicazioni o conversazioni»; ma non anche «la descrizione delle modalità di registrazione», come richiesto dalla prima frase del medesimo articolo in merito alle intercettazioni senza captatore.

Ciò spiega perché la Corte di cassazione, in varie occasioni, abbia osservato che la difesa potrebbe «avere conoscenza solo del verbale delle operazioni di cui all'art. 268 c.p.p. e delle registrazioni, ma non anche dei mezzi tecnici, *hardware* e *software*, utilizzati per l'intrusione nelle conversazioni intercettate, o per decodificare il contenuto»[95].

Sono vari, a dire il vero, gli interessi a giustificazione della segretezza delle chiavi di decriptazione utilizzate in talune tipologie di indagini informatiche, come quelle adottate nel caso *Sky ECC*:

- l'esigenza di tutelare l'efficacia investigativa, evitando che tali chiavi finiscano nelle mani di organizzazioni criminali, e siano magari utilizzate per rendere le proprie comunicazioni ancora più inaccessibili da parte degli organi inquirenti;

- l'esigenza di proteggere il segreto industriale delle aziende proprietarie di quelle chiavi;

- l'esigenza di salvaguardare la sicurezza nazionale, specie laddove venga apposto il segreto di Stato[96].

È innegabile, però, la compressione del diritto di difesa suscettibile di derivarne[97]. Nè vanno sottovalutati gli effetti nefasti per lo stesso accertamento dei fatti generabili

[95] Cfr., ad esempio, Cass., sez. VI, 11 ottobre 2023, n. 48838.

[96] Questi interessi sono posti in rilievo, in particolare, dalla Corte europea dei diritti dell'uomo in rapporto a casi simili alla vicenda *Sky ECC*: cfr. Corte eur., 26 settembre 2023, *Yüksel Yalçinkaya c. Turchia*, § 308. In senso analogo, a livello interno, in rapporto alla mancata comunicazione delle chiavi di decriptazione dei messaggi trasmessi tramite il sistema *Blackberry*, v. Cass., sez. VI, 27 novembre 2018, n. 275534.

[97] Cfr., in riferimento al sistema *Blackberry*, A. GAITO, *Comunicazioni criptate ed esigenze difensive (da Blackberry a Sky-ECC)*, in *Arch. pen. online*, f. 1, 2024, pp. 5 s.; L. FILIPPI, *Questioni nuove in tema di intercettazioni: quid iuris sul "pin to pin" dei Blackberry?*, in *Arch. pen. online*, f. 2, 2016, pp. 3 ss. La questione non è direttamente affrontata dalla disciplina del nuovo strumento dell'ordine di produzione europeo, introdotto dall'UE con il regolamento 1543/2023 del 12 luglio 2023 (la cui entrata in vigore è prevista per il 18 agosto 2026).

dall'omessa *discovery*. Le prove digitali potrebbero apparire perfettamente integre; ma un'erronea decriptazione potrebbe averne alterato il contenuto, e l'indisponibilità degli algoritmi utilizzati potrebbe rendere difficile scoprirlo.

L'opacità delle tecniche informatiche adottate, in particolare, si trova in rotta di collisione con il diritto della difesa di svolgere le proprie osservazioni in merito all'acquisizione e al valore delle prove digitali raccolte all'estero, individuato dalla Corte di giustizia dell'Unione Europea.

Si tratta di un diritto la cui negazione, come abbiamo visto, genera un'inutilizzabilità[98]. Non vi è uniformità di vedute, nondimeno, in merito ai presupposti operativi e alla portata di tale divieto.

9.1. La tesi dell'inutilizzabilità radicale.

In base ad una prima tesi, l'omessa comunicazione alla difesa delle chiavi di decriptazione determinerebbe l'inutilizzabilità radicale delle prove[99].

Tale interpretazione ha senz'altro il pregio di offrire la massima protezione possibile del diritto al contraddittorio tecnico sulla raccolta delle prove digitali.

Si deve, però, essere consapevoli del fatto che un divieto probatorio del genere porrebbe di fronte ad una scelta irragionevole: la rivelazione degli algoritmi, con il conseguente rischio di pregiudicare gli interessi che, come si è detto, possono trovarsi a supporto della loro secretazione; oppure l'inutilizzabilità delle prove, con la conseguente vanificazione delle attività istruttorie e la possibile impunità delle condotte criminose.

Mi sembra che, in entrambi i casi, la tutela del diritto di difesa avverrebbe ad un costo eccessivo, non consentendo di raggiungere il giusto contemperamento fra i valori in gioco.

9.2. L'approccio delle Sezioni Unite: la presunzione relativa di non alterazione delle prove digitali.

La Corte di cassazione, nell'intento di evitare che l'inutilizzabilità di cui si discute portasse a pregiudicare le esigenze di accertamento dei reati, nel caso *Sky ECC* ha adottato un approccio di segno opposto.

Le Sezioni Unite hanno, infatti, ritenuto utilizzabili i messaggi digitali trasmessi dalle autorità francesi, nonostante l'omessa comunicazione degli algoritmi, avvalendosi di un argomento già impiegato in rapporto alla decriptazione dei messaggi scambiati

---

Quest'ultimo è un meccanismo pensato per agevolare le autorità investigative, creando l'obbligo a carico dei *service provider* di mettere a disposizione dell'accusa delle prove digitali in loro possesso, salva la presenza delle eccezioni elencate dall'art. 12 del regolamento.

[98] *Supra*, § 8.6.1.

[99] In questo senso, v. P. TROISI, *I canali di ingresso delle intercettazioni assunte e decrittate all'estero*, in *Proc. pen. giust.*, f. 6, 2024, pp. 1604 ss. Cfr. anche, in rapporto al sistema di messaggistica *Blackberry*, A. GAITO, *Comunicazioni criptate*, cit., pp. 6 ss.

tramite il sistema *Blackberry*[100]: l'impossibilità per la difesa di conoscere le chiavi informatiche utilizzate dall'autorità giudiziaria straniera per la decifrazione delle comunicazioni – si legge nei principi di diritto – «non» determinerebbe, «almeno in linea di principio, una violazione di diritti fondamentali»; «il pericolo di alterazione dei dati» «non» sussisterebbe, «salvo specifiche allegazioni di segno contrario», in quanto «il contenuto di ciascun messaggio» sarebbe «inscindibilmente abbinato alla sua chiave di cifratura», per cui «una chiave errata non» avrebbe «alcuna possibilità di decriptarlo, anche solo parzialmente»[101].

Nelle parole della Procura Generale, «o il messaggio è decrittato attraverso l'unico codice possibile o rimane una stringa alfanumerica priva di significato, cioè criptata: si deve escludere che si possa decifrarne una parte corretta e una non corretta; né vi sono possibilità che una chiave errata possa decrittare il contenuto, anche parziale, del codice umano contenuto»[102].

In questa visione, dunque, l'intellegibilità delle prove digitali sarebbe un segnale sicuro del fatto della loro mancata alterazione; diversamente, qualora fosse stata impiegata una tecnica di decriptazione scorretta, il loro contenuto sarebbe incomprensibile.

L'assunto non è presentato come inconfutabile, ma riveste la forma della presunzione relativa: dovrebbe essere, cioè, la parte interessata a fornire l'eventuale prova contraria. Come osserva la Procura generale, «resta ferma la possibilità per la difesa di dedurre, sulla base di ragioni specifiche, anomalie tecniche in grado di fare dubitare della correttezza delle acquisizioni e dell'inquinamento del risultato probatorio e, in tal caso, il correlativo obbligo, per l'autorità giudiziaria, di promuovere accertamenti sul punto». Ad esempio, tramite l'allegazione in giudizio foto dello schermo del criptofonino da cui emergano difformità rispetto ai messaggi estrapolati dalle autorità giudiziarie[103].

È un'impostazione che, a mio modo di vedere, presta il fianco ad obiezioni.

In primo luogo, si tratta di una presunzione che appare troppo semplicistica. Può essere statisticamente vero che la comprensibilità dei messaggi sia un segnale della correttezza delle tecniche informatiche utilizzate per ottenerli. Ma non è da escludere che, in determinate situazioni, questa correlazione venga meno, a causa dell'impiego di metodi di alterazione dei messaggi tali da non lasciare traccia: tutto dipende dalle specificità di ciascuna situazione concreta. La perentorietà del principio di diritto della Sezioni Unite rischia di creare un corto circuito valutativo, inibendo gli approfondimenti che si rendessero, volta per volta, necessari[104].

---

[100] Cfr. Cass., sez. VI, 27 novembre 2018, n. 14395.

[101] Sentenza *Gjuzi*, § 12.4; sentenza *Giorgi*, § 18.5.3.

[102] *Memoria* della Procura generale, p. 72

[103] *Memoria* della Procura generale, p. 71.

[104] In senso analogo, cfr. A. GAITO, *Comunicazioni criptate*, cit., pp. 3 ss., in rapporto ai messaggi scambiati attraverso il servizio *Blackberry*.

Né va trascurato che la presunzione delineata dalle Sezioni Unite determina una notevole compressione del diritto di difesa[105]: per quanto configurata come relativa, in molti casi essa si converte, nella sostanza, in una presunzione assoluta, poichè senza la conoscenza delle chiavi di decriptazione sarebbe piuttosto difficile fornire la prova contraria.

9.3. I margini di utilizzabilità dei messaggi decriptati: l'onere motivazionale del giudice italiano.

Credo che sia necessario partire dalla premessa per cui la questione non vada affrontata con un approccio rigido. Sarebbe irragionevole applicare l'onere della prova a carico di chi vorrebbe eccepire l'inutilizzabilità di cui si discute in modo meccanicistico, così come affermano le Sezioni Unite, trascurando le difficoltà connesse all'opacità che la raccolta delle prove digitali è suscettibile di assumere.

Sono chiare, del resto, le spinte delle corti sovranazionali nel senso dell'adozione di una prospettiva flessibile, che portano a calibrare la presenza del divieto probatorio sulla scorta di una logica caso per caso.

Lo si evince, *in primis*, dalla sentenza *Encrochat* della Corte di giustizia, secondo la quale il diritto ad interloquire in relazione all'acquisizione e alla valutazione dei messaggi digitali dovrebbe possedere il requisito dell'"efficacia": una connotazione non certo univoca[106], che fa comprendere come esso potrebbe essere compresso in misura maggiore o minore a seconda della singola vicenda.

Indicazioni ancora più specifiche provengono dalla decisione della Corte europea dei diritti dell'uomo *Yüksel Yalçinkaya*, relativa ad una persona condannata per aver partecipato al tentato colpo di stato avvenuto in Turchia nel 2016 sulla base di messaggi scambiati tramite un servizio di messaggistica crittografata denominato *ByLock*. Il diritto dell'accusato alla *discovery* delle modalità di svolgimento e dei risultati delle indagini, qui, non è configurato in modo assoluto, ma viene bilanciato con le esigenze contrapposte[107].

Se ne può ricavare, secondo i giudici di Strasburgo, un "onere rafforzato" in capo ai giudici nazionali di individuare le ragioni che giustificano l'impossibilità per la difesa di avere accesso alle prove o, comunque, di verificarne l'integrità e l'attendibilità[108].

Di qui un obbligo motivazionale che, comunque, può essere fatto discendere dal principio di proporzionalità che, come abbiamo visto, deve guidare anche la raccolta transnazionale delle prove[109]. Non a caso, l'art. 7 d.lgs. 108/2017 prescrive che l'OEI non

---

[105] Cfr. L. MARAFIOTI, *Sezioni unite e tirannie tecnologiche: diritto di difesa, contraddittorio e "criptofonini"*, in *dirittodifesa.eu*, 18 settembre 2024, § 4, secondo cui l'argomento delle Sezioni Unite sarebbe viziato da "tirannia tecnologica".

[106] Si veda E. LORENZETTO, *Il caso* Encrochat *e l'ordine europeo di indagine penale nella staffetta fra corte di giustizia e diritto dello stato di emissione*, in *Cass. pen.*, 2024, p. 2895.

[107] Cfr. Corte eur., 26 settembre 2023, *Yüksel Yalçinkaya c. Turchia*, § 306 s. In merito all'approccio della Corte europea v. J.J. OERLEMANS-D.A.G. VAN TOOR, *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, in *Eur. Journ. Crime Crim. Law Crim Just.*, f. 30, 2022, pp. 321 ss.

[108] Corte eur., 26 settembre 2023, *Yüksel Yalçinkaya c. Turchia*, § 334.

[109] *Supra*, § 8.2.

sarebbe proporzionato se dalla sua esecuzione potesse derivare un sacrificio per i diritti «non giustificato dalle *esigenze* investigative o probatorie del *caso concreto*».

Ma quali parametri il giudice dovrebbe impiegare per stabilire se il sacrificio in questione sia stato di entità tale da generare il divieto probatorio di cui di discute? Dal *case-law* della Corte di giustizia e della Corte europea emergono vari indici di violazione del diritto di difesa e dell'equità processuale, che possono essere utilmente impiegati a tal scopo.

a) Influenza preponderante delle prove

Una prima condizione, individuata dalla Corte di giustizia, è che l'impiego delle prove possa «influenzare in modo preponderante la valutazione dei fatti»[110].

Applicato alla lettera, tale requisito presupporrebbe che le prove raccolte all'estero sarebbero inutilizzabili solo quando fossero fornite di un valore conoscitivo superiore a quello delle altre prove.

In questo modo, però, la questione della loro ammissibilità verrebbe a sovrapporsi a quella della loro valutazione, confondendo tra loro due momenti del procedimento probatorio che dovrebbero rimanere distinti.

Sarebbe, inoltre, un presupposto difficile da definire, se si considera che la logica che governa la ricostruzione dei fatti impedisce di quantificare il peso delle prove in modo preciso[111]. Entro quali limiti le prove raccolte all'estero potrebbero ritenersi preponderanti qualora trovassero riscontro in altre prove? Quanto dovrebbero essere solidi i riscontri per affermare che quelle prove non sarebbero tali? Stiamo parlando, come è agevole comprendere, di un giudizio discrezionale, suscettibile di creare incertezze e disparità di trattamento tra casi simili.

Volendo attribuire al parametro in questione un contenuto più oggettivo, è preferibile ritenere che esso stia, semplicemente, ad indicare che le prove raccolte all'estero dovrebbero avere un autonomo rilievo nel ragionamento inferenziale a fondamento della ricostruzione dei fatti; dovrebbe, cioè, trattarsi di prove da cui il giudice possa trarre elementi utili nella costruzione delle catene induttive che collegano le prove acquisite con i fatti da provare[112].

Non sfugge, naturalmente, come il requisito, così inteso, diventi del tutto superfluo, venendo a coincidere con il vaglio di rilevanza previsto dall'art. 190 c.p.p.

b) Valori protetti dall'omessa discovery

Un autentico requisito di cui tenere conto per stabilire se le prove siano utilizzabili o no consiste, piuttosto, nell'evenienza che la secretazione degli algoritmi di decriptazione persegua uno degli interessi meritevoli di tutela più sopra considerati[113].

---

[110] V. *supra*, § 8.6.

[111] Definisce "evanescente" tale criterio G. SPANGHER, *La Corte di Giustizia e i criptofonini*, in *giustiziainsieme.it*, 6 maggio 2024.

[112] In senso analogo, v. O. CALAVITA, *L'ordine europeo*, cit., p. 271.

[113] *Supra*, § 9.

c) Stretta necessità

La limitazione della *discovery* dovrebbe, poi, risultare "strettamente necessaria" ai fini della salvaguardia degli interessi in questione[114].

Il giudice dovrebbe, dunque, individuare le ragioni a sostegno di tale stretta necessità, spiegando perché non ci sarebbero alternative alla secretazione delle chiavi di decriptazione.

d) Misure di controbilanciamento

Le restrizioni imposte alla difesa, infine, dovrebbero essere «sufficientemente controbilanciate» dalle «procedure seguite dalle autorità giudiziarie»[115].

Tali fattori di compensazione non potrebbero essere determinati in astratto, ma andrebbero individuati caso per caso. Ad esempio, il mancato accesso agli algoritmi potrebbe essere surrogato da una particolare diligenza da parte degli organi investigativi nel mettere a disposizione della difesa tutti gli elementi raccolti nel corso delle investigazioni, compresi quelli a discarico.

e) Obbligo logico di riscontri

Se ritenute utilizzabili, le prove digitali decriptate in base a tecniche non conoscibili dalla difesa dovrebbero essere valutate tenendo conto del fatto che potrebbero essere state oggetto di alterazioni tali da non emergere a vista d'occhio.

A questo fine, pur in assenza di una previsione quale quella dell'art. 192 comma 3 c.p.p., il giudice, per evitare di incorrere in un vizio di motivazione, non potrebbe esimersi dall'andare alla ricerca di elementi di riscontro nel restante materiale probatorio, in modo da compensare i potenziali *deficit* cognitivi di elementi non vagliati attraverso il pieno contraddittorio tecnico.

Chiaramente, più le lacune informative risultassero gravi, più aumenterebbero le difficoltà per il giudice di ritenere soddisfatto lo *standard* dell'accertamento della colpevolezza al di là di ogni ragionevole dubbio. Il che dimostra come, in una certa misura, il rischio della mancata prova della correttezza delle tecniche informatiche impiegate gravi anche sull'accusa[116].

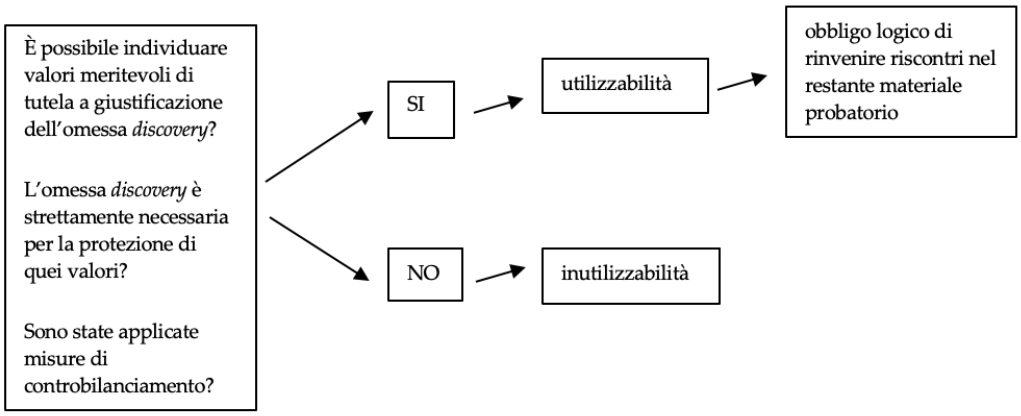
---

[114] Corte eur., 26 settembre 2023, *Yüksel Yalçinkaya c. Turchia*, § 308.

[115] Corte eur., 26 settembre 2023, *Yüksel Yalçinkaya c. Turchia*, § 308.

[116] In senso analogo, in rapporto alla prova genetica, v. Corte di assise d'appello di Perugia, 3 ottobre 2011, *Knox e Sollecito*, in *giurisprudenzapenale.com*, p. 83, secondo cui sussisterebbe l'onere dell'accusa di provare che i risultati probatori sono stati ottenuti mediante un «un procedimento che garantisca la genuinità del reperto dal momento della refertazione a quello dell'analisi». V. P. TONINI, Nullum iudicium sine scientia. *Cadono vecchi idoli nel caso* Meredith Kercher, in *Dir. pen proc*., 2015, pp. 1414 ss.

In sintesi, i requisiti di utilizzabilità appena considerati si possono così rappresentare.



Proprio in applicazione di questo schema argomentativo, nel caso *Yüksel Yalçinkaya c. Turchia* la Corte europea aveva riconosciuto la violazione del diritto all'equo processo, identificando gravi carenze informative non adeguatamente controbilanciate:

- l'accusato non era mai stato messo nelle condizioni di sottoporre a verifica il contenuto e l'integrità dei dati digitali rinvenuti dagli organi inquirenti nella piattaforma *ByLock*; le richieste avanzate dalla difesa a tale riguardo erano rimaste senza esito;
- in particolare, non era stata data nessuna risposta a talune difformità emerse in rapporto all'individuazione dell'identità e del numero degli utenti i cui messaggi erano stati captati;
- il contenuto decriptato dei messaggi e le generalità dei loro destinatari non erano mai stati messi a disposizione della difesa;
- tutte queste limitazioni non erano state adeguatamente motivate dalle autorità giudiziarie;
- neppure erano state ben delineate le ragioni per cui i messaggi erano stati ritenuti sufficientemente attendibili[117].

Segnali di questo approccio si colgono anche a livello nazionale. Basti pensare ad una decisione con cui la Corte di cassazione, anche se con un ragionamento meno strutturato di quello della Corte europea, ha annullato il provvedimento di conferma di un'ordinanza applicativa della custodia cautelare in carcere emessa da un tribunale del riesame, per la ragione che quest'ultimo aveva ritenuto del tutto «ininfluente» accertare le modalità con cui l'autorità straniera aveva acquisito e decriptato le conversazioni intercorse fra gli indiziati[118].

[117] Cfr. Corte eur., 26 settembre 2023, *Yüksel Yalçinkaya c. Turchia*, § 327 s.
[118] Cfr. Cass., sez. I, 12 marzo 2024, n. 13535.

10. Un'incessante guerra informatica.

Nel caso *Sky ECC*, la classica contrapposizione fra la tutela dei diritti fondamentali e la salvaguardia delle esigenze investigative si è innestata in un contesto tecnologico complesso, che ha reso ancora più problematico individuare il corretto punto di equilibrio fra i valori in gioco.

È una vicenda da cui si può senz'altro trarre l'insegnamento di cercare di evitare gli estremismi.

È necessario, da un lato, sfuggire alle trappole cognitive generate dalle prove digitali: le quali spesso risultano ingannevoli, e per tale ragione devono essere valutate unitamente al contesto da cui traggono origine, considerandone le modalità di acquisizione e i potenziali rischi.

Né si deve cadere nella tentazione di impiegare in modo scriteriato i nuovi metodi investigativi consentiti dalle tecnologie informatiche, dotati di capacità intrusive senza precedenti. Il loro uso va calibrato nei limiti della stretta necessità, dando sempre la preferenza alle modalità meno invasive.

Sarebbe eccessivo, d'altro lato, adottare un approccio volto a sanzionare con l'inutilizzabilità qualunque forma di compressione dei diritti determinata dalle indagini informatiche.

Le prove digitali, proprio perché prive di corporeità, sono inevitabilmente più sfuggenti ed opache rispetto alle tradizionali prove fisiche. Ciò non rende sempre possibile, allo stato delle cose, una totale trasparenza in relazione alle modalità con cui esse vengono acquisite ai fini investigativi. Il giudice deve essere consapevole del fatto che alcuni loro aspetti potrebbero rimanere nell'ombra, e trarne le dovute conseguenze, se non altro, al momento della valutazione.

Oltretutto, la loro collocazione in enormi luoghi virtuali pieni di informazioni di ogni genere, magari altamente sensibili, di fatto rende impossibile la loro apprensione senza interferire con il diritto alla riservatezza. Concludere che sarebbero inutilizzabili per questa sola ragione significherebbe aprire dei comodi spazi di impunità per le organizzazioni criminali.

Anche perché non va trascurato che vicende come quelle di *Sky ECC* rappresentano solo singole battaglie nel contesto di un'incessante guerra tecnologica fra la criminalità e gli organi investigativi[119]. La prima, grazie anche alle risorse offerte dall'intelligenza artificiale, riuscirà a trovare metodi sempre diversi per nascondere le proprie comunicazioni. I secondi dovranno continuamente adeguarsi, percorrendo vie inedite per rompere il velo della criptazione evitando di compromettere in modo irreparabile il diritto alla riservatezza, le garanzie difensive e l'attendibilità delle prove acquisite.

[119] Cfr. S. RAGAZZI-F. SPIEZIA, *Decifrare, acquisire e utilizzare le comunicazioni criptate*, cit., pp. 227 ss.