DIRITTO di DIFESA
GIUFFRÈ FRANCIS LEFEBVRE LA RIVISTA DELL'UNIONE DELLE CAMERE PENALI ITALIANE

SEZIONI UNITE E TIRANNIE TECNOLOGICHE: DIRITTO DI DIFESA, CONTRADDITTORIO E "CRIPTOFONINI"*

di *Luca Marafioti*

SOMMARIO: 1. Attività investigative digitali *ultra fines* su dispositivi criptati. – 2. Disorientamenti giurisprudenziali sull'acquisizione dei dati digitali criptati. - 3. Il ragionamento ipotetico delle Sezioni Unite. – 4. Crittografia e contraddittorio in rotta di collisione.

1. Attività investigative digitali *ultra fines* su dispositivi criptati

Con le sentenze n. 23755/24[1] e n. 23756/24[2], le Sezioni Unite sono state chiamate a pronunciarsi, tra l'altro, sulle regole e sulle garanzie che devono presidiare l'acquisizione dei dati digitali estratti da un *server* collocato all'estero per mano dell'autorità giudiziaria di quello Stato[3].

I dati digitali in discorso sono quelli contenuti nei "criptofonini", vale a dire *smartphone* tecnologicamente avanzati e dotati di particolari funzioni a tutela della riservatezza dell'utilizzatore, quali elevati *standard* crittografici e accorgimenti tali da renderli impenetrabili ai più moderni mezzi di

*Il presente lavoro riproduce, con alcune integrazioni e l'aggiunta di note essenziali, il testo di un intervento tenuto nel corso dell'Incontro su "*L'acquisizione della messaggistica digitale e delle chat. Questioni processuali, tutela della corrispondenza e garanzie europee*", tenutosi il 20 giugno 2024, su iniziativa della Camera Penale di Milano – Gian Domenico Pisapia.

[1] Cass., Sez. Un., 29 febbraio 2024, Gjuzi, in *C.E.D. Cass.*, rv. 286573.

[2] Cass., Sez. Un., 29 febbraio 2024, Giorgi, in *C.E.D. Cass.*, rv. 286589.

[3] Per un commento a prima lettura sulle pronunce in discorso, v. M. DANIELE, *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini*, in www.sistemapenale.it, 17 luglio 2024.

ricerca della prova digitale[4]. Proprio in ragione dell'impossibilità per gli investigatori di accedere al contenuto della strumentazione digitale in esame attraverso gli ordinari strumenti investigativi, l'unica possibilità per acquisire i dati ivi custoditi è riuscire a penetrare, tramite un'operazione di *hacking*, nel *server* che li contiene.

Sotto quest'angolo visuale, le attività acquisitive dei dati digitali criptati contenuti nei criptofonini si inquadrano agevolmente nel più ampio tema delle indagini *ultra fines* in materia di prova digitale[5]. Si tratta, come noto, di questione dipendente dal carattere intrinsecamente aterritoriale della *digital evidence*. Ai dati digitali si può accedere, mediante la rete *Internet*, da qualunque luogo, a prescindere dalla effettiva collocazione territoriale "fisica" del *server* che custodisce il dato[6].

Nel caso di specie, un'autorità giudiziaria europea era, appunto, riuscita a superare ogni ostacolo.

Dapprima si era introdotta da remoto nei *server* che custodivano i dati dei criptofonini e, successivamente, a decrittarli. Si badi: il tutto secondo modalità non note, giacché sulle medesime è stato apposto il segreto di Stato, ma con ogni probabilità attraverso l'uso di un *trojan horse*[7].

Dell'esistenza di tali dati, poi, sono state informate le varie autorità giudiziarie – tra cui quella italiana – che avrebbero potuto avere interesse ad una loro acquisizione a fini processuali; acquisizione infine avvenuta tramite lo strumento dell'ordine europeo d'indagine.

Sulla legittimità di tale acquisizione si appuntavano le doglianze formulate dai ricorrenti in due distinti procedimenti giunti allo scrutinio della Corte di cassazione. In estrema sintesi e per quanto di

---

[4] Sulle questioni processuali legate all'avvento dei criptofonini, v. D. CURTOTTI-V. RIZZI-W. NOCERINO-A.M. RUSSITTO-G. GILIBERTI-G. SCARPA, *Piattaforme criptate e prova penale*, in *Sist. pen.*, 2023, n. 6, p. 173 ss.; L. LUDOVICI, *I criptofonini: sistemi informatici criptati e server occulti*, in www.penaledp.it, 14 ottobre 2023; M. RAMPIONI, *I limiti di utilizzabilità della messaggistica criptata SkyEcc acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali*, in *Giur. pen.* web, 2023, n. 10, 25 ottobre 2023; 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 *Sist. pen.*, 2024, n. 2, p. 203 ss.; A. GAITO, *Comunicazioni criptate ed esigenze difensive (da Blackberry a Sky-ECC)*, in *Arch. pen.*, 2024, n. 1, 31 maggio 2024; L. MASSARI, *Il diritto di difesa, questo sconosciuto: il caso dei criptofonini e degli ordini europei di indagine*, in *Dir. dif.*, 11 settembre 2024.

[5] In proposito, v. F. SIRACUSANO, *La prova digitale transnazionale: un difficile "connubio" tra innovazione e tradizione*, in *Proc. pen. giust.*, 2017, n. 1, p. 178 ss.; M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (a cura di), *Cybercrime. Diritto e procedura penale dell'informatica*, Utet, 2018, p. 1621 ss.; M. PITTIRUTI, *L'apprensione all'estero della prova digitale*, in L. LUPÁRIA-L. MARAFIOTI-G. PAOLOZZI (a cura di), *Dimensione tecnologica e prova penale*, Giappichelli, 2019, p. 205 ss.; , D. CURTOTTI, *Indagini* hi-tech*, spazio* cyber*, scambi probatori tra Stati e Internet provider service e "Vecchia Europa": una normativa che non c'è (ancora)*, in *Dir. pen. proc.*, 2021, p. 745 ss.; G. DI PAOLO, *La circolazione transfrontaliera delle prove elettroniche*, in www.penaledp.it, 13 maggio 2024.

[6] Sul tema, in chiave monografica, cfr. M. PITTIRUTI, Digital Evidence *e procedimento penale*, Giappichelli, 2017, *passim* e spec. p. 6 ss., nonché S. SIGNORATO, *Le indagini digitali: profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, *passim*. Cfr., altresì, volendo, L. MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, in *Cass. pen.*, 2011, p. 4509 ss.

[7] Sul tema, volendo, v. L. MARAFIOTI, Trojan horse: *spiragli di retromarcia legislativa*, in www.questionegiustizia.it, 24 gennaio 2023.

interesse in questa sede, un primo ordine di censure riguardava, per un verso, la ritenuta possibilità di applicare la disciplina di cui all'art. 234-*bis* c.p.p. ai dati informatici relativi alle comunicazioni intercorse tramite i criptofonini; nonché, per altro verso, la menomazione del diritto di difesa causata dalla mancata ostensione alla difesa delle tecniche di acquisizione e di decrittazione dei dati.

Un secondo ordine di censure si incentrava sull'inutilizzabilità dei dati digitali recuperati dall'autorità estera.

Ciò per una duplice ragione: da un lato, per violazione dell'art. 6, par. 1, lett. *a*) e *b*) della Direttiva 2014/41/UE, giacché frutto di attività investigative che mai, in un caso analogo, avrebbero potuto essere compiute in Italia; dall'altro lato, per violazione dell'art. 14 Cost, in quanto le chiavi crittografiche sarebbero state recuperate per mezzo di captatori informatici, in assenza di una loro disciplina legislativa e, dunque, in violazione della riserva di legge prevista dalla Costituzione.

Preso atto delle oscillazioni giurisprudenziali in materia, due Sezioni singole della Suprema Corte rimettevano con due distinte ordinanze i ricorsi alle Sezioni Unite. Segnatamente, l'ordinanza n. 47798/23[8] sottoponeva alle Sezioni Unite due questioni di diritto, relative l'una all'inquadramento dogmatico dell'acquisizione di messaggi su *chat* di gruppo, scambiati su sistema cifrato, mediante ordine europeo d'indagine e l'altra alla necessità o meno di una verifica giurisdizionale in Italia – preventiva o successiva – sulla legittimità dell'acquisizione dei dati digitali. Dal canto suo, l'ordinanza n. 2329/24[9] reiterava quest'ultima questione e ve ne aggiungeva un'altra, circa la possibilità di ricondurre alla fattispecie di cui all'art. 270 c.p.p. l'acquisizione, mediante ordine europeo d'indagine, dei dati digitali criptati.

All'esito, le Sezioni Unite hanno enunciato ben sei principi in sede di interpretazione della legge processuale: *in primis*, l'acquisizione dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera in un procedimento penale pendente davanti ad essa ed effettuate su una piattaforma informatica criptata è assoggettata alla disciplina di cui all'art. 270 c.p.p.; in secondo luogo, le prove già in possesso delle autorità competenti dello Stato di esecuzione possono essere legittimamente richieste ed acquisite dal pubblico ministero italiano mediante emissione di ordine europeo d'indagine senza necessità di preventiva autorizzazione giudiziale; inoltre, l'emissione di ordine europeo d'indagine diretto ad ottenere i risultati di intercettazioni disposte da un'autorità giudiziaria straniera, effettuate

[8] Cass., Sez. III, ord. 3 novembre 2023, Gjuzi, in www.italgiure.giustizia.it.
[9] Cass., Sez. VI, ord. 15 gennaio 2024, Giorgi, in www.italgiure.giustizia.it.

attraverso l'inserimento di un captatore informatico sui *server* di una piattaforma criptata, poi, è ammissibile e non va preceduta da una richiesta di autorizzazione al giudice; in materia di *data retention*, il pubblico ministero è tenuto a richiedere l'autorizzazione al giudice solo in sede di primo accesso al dato, ma non anche in caso di circolazione probatoria dei tabulati; ancora, il giudice del procedimento di destinazione del materiale probatorio trasmesso dall'estero è tenuto a dichiarare l'inutilizzabilità delle prove se, in relazione ad esse, si sia verificata la violazione dei diritti fondamentali, ma l'onere di allegare e provare i fatti da cui inferire tale violazione grava sulla parte interessata; infine, il mancato accesso all'algoritmo impiegato per decriptare i dati digitali non determina alcuna violazione dei diritti fondamentali in capo alla difesa, salvo specifiche allegazioni di segno contrario.

2. Disorientamenti giurisprudenziali sull'acquisizione dei dati digitali criptati

Nella giurisprudenza, sulle questioni sottoposte allo scrutinio delle Sezioni Unite si contendono il campo, al netto di qualche inevitabile semplificazione, due principali orientamenti.

Una prima linea di pensiero ritiene che, per la trasmissione di materiale probatorio digitale costituito da comunicazioni svolte attraverso *chat* criptate e già in possesso di un'autorità giudiziaria estera, il pubblico ministero non sia tenuto ad ottenere alcuna previa autorizzazione giudiziale[10], né occorra alcun controllo successivo da parte del giudice italiano.

Alcune sentenze sono pervenute a tale conclusione valorizzando la previsione di cui all'art. 234-*bis* c.p.p.[11], ai sensi del quale è «sempre consentita» – e dunque non occorrerebbe verifica alcuna in sede giurisdizionale – l'acquisizione di dati digitali conservati all'estero e non disponibili al pubblico, qualora il «legittimo titolare» presti il suo consenso. Il legittimo titolare dovrebbe identificarsi con il soggetto che di quei dati può disporre in forza di un qualsiasi "titolo" legittimo, ivi compreso colui che quel dato

[10] Spesso l'assunto è giustificato con il rilievo secondo cui il pubblico ministero italiano sarebbe dotato dei caratteri di autonomia e indipendenza: cfr. Cass., Sez. IV, 11 maggio 2023, Bonifazio, in www.italgiure.giustizia.it. In dottrina, in chiave critica sull'ibrida configurazione di parte *sui generis* del pubblico ministero, cfr., da ultimo, R. DEL COCO, *La maschera e il volto della consulenza tecnica*, in *Proc. pen. giust.*, 2021, n. 3, p. 669 ss.

[11] V. Cass., Sez. I, 1° luglio 2022, Molisso, in www.italgiure.giustizia.it; Cass., Sez. I, 13 ottobre 2022, Calderon, in *Cass. pen.*, 2023, p. 2784 ss., con nota di W. NOCERINO, *L'acquisizione della messaggistica su sistemi criptati: intercettazioni o prova documentale?*; Cass., Sez. I, 13 ottobre 2022, Minchino, in www.italgiure.giustizia.it; Cass., Sez. IV, 5 aprile 2023, Papalia, in *Proc. pen. giust.*, 2023, n. 6, p. 1318 ss., con nota di M. PASCAZIO, *Nessun dietrofront sull'utilizzabilità della messaggistica decriptata da autorità giudiziaria straniera*, nonché in www.penaledp.it, 23 giugno 2023, con nota di L. FILIPPI, *Criptofonini e diritto di difesa*; Cass., Sez. IV, 5 aprile 2023, Liguori e al., in www.italgiure.giustizia.it; Cass., Sez. IV, 30 maggio 2023, Iannaci, *inedita*.

ha acquisito al fine di accertare reati. Per tale via, soggetti legittimati sarebbero anche la polizia giudiziaria e l'autorità giudiziaria dello Stato estero[12].

Al medesimo fine di sostenere la piena legittimità dell'acquisizione del materiale probatorio digitale già "recuperato" dall'autorità giudiziaria estera, si è fatto leva, altresì, sulle regole in materia di ordine europeo d'indagine. In quest'ottica, i giudici di legittimità hanno evidenziato che sarebbe sufficiente l'intervento di un giudice nel corso della procedura estera acquisitiva della prova, ovverossia nello Stato ove la prova è stata raccolta[13].

In prospettiva analoga, più di recente, si è evidenziato che, nel sistema giuridico italiano, per l'acquisizione di comunicazioni personali conservate nei dispositivi informatici, anche quando queste costituiscano corrispondenza, si applicano le regole in materia di perquisizione e sequestro. Valgono, insomma, le previsioni contenute negli artt. 244, 247, comma 1-*bis,* 254-*bis* e 352, comma *1-bis,* c.p.p., le quali non prescrivono l'intervento di un giudice[14]. Del resto, trattandosi di documenti, un controllo *ex post* da parte del giudice italiano dovrebbe comunque escludersi, in ragione della disciplina per l'acquisizione del mezzo di prova in discorso.

Per converso, qualora i dati digitali d'interesse siano il frutto di un'attività di captazione di comunicazioni, la superfluità di un'autorizzazione del giudice si ricaverebbe dall'art. 270 c.p.p. La lettera della disposizione, che impone limiti alla circolazione delle intercettazioni correlati soltanto alla gravità del reato da accertare nel procedimento di destinazione, consentirebbe di teorizzare una "libera" trasmigrazione delle captazioni, senza alcuna necessità di autorizzazione né di controllo successivo ad opera di un giudice[15].

Indirizzato in senso più garantista è, invece, il diverso orientamento, secondo cui l'acquisizione di messaggi su *chat* di gruppo scambiati con sistema cifrato, effettuata mediante un ordine europeo di indagine, quando attiene ai risultati di un'apprensione occulta di comunicazioni non in corso o di un sequestro di dati archiviati in un *server*, è regolata dalla disciplina codicistica relativa ai mezzi di ricerca della prova digitale e, precipuamente, dall'art. 254-*bis* c.p.p.

---

[12] Il ragionamento è ripreso anche da Cass, Sez. VI, 28 marzo 2023, Gulluni, in *Giur. it.*, 2023, p. 2191 ss., con nota di M.T. MORCELLA, Da mihi factum, dabo tibi ius: *un principio irrinunciabile, pure nell'era dei criptofonini*. Alla pronuncia si deve la precisazione in base alla quale, in ogni caso, dal mancato consenso della società di gestione del *server* non scaturisce la violazione di una norma inderogabile o di un principio fondamentale del nostro ordinamento, giacché l'art. 234-*bis* c.p.p. è «norma processuale interna, che non si identifica necessariamente con i principi fondamentali del nostro ordinamento».
[13] Cfr. Cass., Sez. I, 13 ottobre 2022, Calderon, cit.; Cass., Sez. I, 13 ottobre 2022, Minchino, cit.
[14] Cass., Sez. VI, 27 settembre 2023, Bruzzaniti, in *C.E.D. Cass.*, rv. 285363.
[15] Cass., Sez. VI, 27 settembre 2023, Bruzzaniti, cit.; Cass., Sez. III, 19 ottobre 2023, Bruzzaniti, in *C.E.D.* Cass. rv. 285350.

Di conseguenza, dovrebbe trovare applicazione la disciplina del sequestro di dati informatici presso fornitori di servizi e non l'art. 234-*bis* c.p.p. Quest'ultima disposizione, invero, farebbe riferimento solo a elementi preesistenti rispetto al momento d'inizio delle indagini. E comunque: il "legittimo titolare" menzionato dalla previsione sarebbe, oltre che la società di gestione della piattaforma di transito della comunicazione, soltanto il mittente o il destinatario del messaggio. Per converso, l'autorità giudiziaria sarebbe mera detentrice del dato.

Quanto all'interrogativo circa la necessità di un provvedimento autorizzativo emesso da un giudice, si fornisce risposta affermativa allorché l'acquisizione riguardi corrispondenza o altre forme di comunicazione, sulla scia dei più recenti approdi della giurisprudenza costituzionale[16] e sovranazionale[17]. L'illegittimità di un ordine europeo d'indagine emesso senza la preventiva autorizzazione del giudice, quando obbligatoria, produrrebbe conseguenze diversificate: se l'ordine d'indagine ha determinato lo svolgimento di un'attività investigativa illegittima, la genesi patologica della prova raccolta ne provocherebbe l'inutilizzabilità; se l'ordine è stato emesso al fine di acquisire una prova già disponibile nello Stato di esecuzione, il giudice italiano dovrebbe operare una verifica sulla sussistenza delle condizioni di ammissibilità della prova[18].

A voler sintetizzare in poche battute le due antitetiche ricostruzioni sin qui ripercorse, può dirsi che la prima tende ad avallare il libero ingresso del materiale probatorio raccolto *ultra fines*, soprattutto mediante un'omologazione tra il dato digitale e l'ampio contenitore della prova documentale; tesi cui fa da corollario una radicale esclusione che un qualsivoglia controllo sulla prova "preconfezionata" possa essere affidato al giudice italiano. In diversificata prospettiva, il secondo orientamento vede negli strumenti interni di reperimento del materiale digitale in fase investigativa gli ineludibili referenti per l'attività di acquisizione dei dati contenuti in un *server*. Di conseguenza, fa dipendere la necessità di un controllo giurisdizionale dalla tipologia di dato da acquisire nella vicenda concreta.

---

[16] Corte cost., sent. 22 giugno 2023 (ud. 7 giugno 2023 – dep. 27 luglio 2023), n. 170/2023, in *G.U.*, 2 agosto 2023, n. 31. Per un commento alla pronuncia, v. F. CERQUA-L. LUPÁRIA DONATI, *La versione della Consulta sulla corrispondenza elettronica. Un* bouleversement *in materia di prova digitale?*, in *Dir. inf.*, 2023, n. 5, p. 718 ss. V. anche Corte cost., sent. 20 dicembre 2022 (ud. 19 dicembre 2022 – dep. 12 gennaio 2023), n. 2/2023, in *G.U.*, 18 gennaio 2023, n. 3.

[17] Corte di Giustizia, Grande Sezione, sent. 2 marzo 2021, H.K. c. Prokuratuur, causa C-746/18.

[18] Cfr. le due sentenze Cass., Sez. VI, 26 ottobre 2023, Iaria e Cass., Sez. VI, 26 ottobre 2023, Kolgjokaj, in *Cass. pen.*, 2024, p. 162 ss., con note di E. LORENZETTO, *L'acquisizione all'estero di comunicazioni digitali criptate nella fucina dell'ordine europeo di indagine penale* e G. SPANGHER, *Criptofonini: sono "in gioco" diritti fondamentali*; in *Arch. pen.* web, 2023, n. 3, 28 novembre 2023, con nota di N. GALLO, *Un altro tassello giurisprudenziale in tema di Ordine Europeo d'Indagine penale (OEI) per l'acquisizione della* digital evidence *dal* server *estero*; in *Penale DP*, 2023, n. 3, p. 483 ss., con nota di W. NOCERINO, *Ancora in tema di criptofonini: nuovi arresti giurisprudenziali in attesa delle Sezioni Unite*.

A prescindere dall'impostazione prescelta, risulta chiaro l'intimo legame tra le due questioni che la Suprema Corte era chiamata ad affrontare: identificare uno strumento processuale da impiegare per l'acquisizione dei dati criptati, dall'angolo visuale del diritto interno, rappresenta quesito evidentemente connesso con quello circa la necessità o meno di una verifica giurisdizionale in ordine alla possibilità d'ingresso di tali dati nella vicenda processuale italiana. La soluzione del secondo quesito dipende, insomma, da quella fornita al primo.

3. Il ragionamento ipotetico delle Sezioni Unite

Occorre ammettere che un'eventuale risposta negativa avrebbe rischiato di aprire la strada ad una duplice conclusione inaccettabile: un'atipicità assoluta della materia combinata con una radicale assenza di controlli. Dietro ai quesiti posti alla Suprema Corte, infatti, si aggira lo spettro di una pericolosa minaccia per l'esercizio del diritto di difesa ed al contraddittorio tecnico.

Cosicché, le risposte fornite dalle Sezioni Unite possono considerarsi una, ancorché assai parziale, smentita alle preoccupazioni legate alle possibili conseguenze in termini di garanzia se solo si fosse avallato un totale "via libera" all'impiego del materiale probatorio.

In effetti, tra gli aspetti positivi della soluzione fatta propria dalle Sezioni Unitesi colloca il netto rifiuto di un possibile utilizzo dell'art. 234-*bis* c.p.p. nel caso di specie. Ciò alla luce della condivisibile argomentazione secondo cui tale disposizione riguarda l'acquisizione di elementi conservati all'estero che prescinde da forme di collaborazione con l'autorità giudiziaria di altro Stato. Collaborazione che, viceversa, impone l'attivazione del diverso strumento dell'ordine europeo d'indagine[19].

Nondimeno, la pronuncia delude nella misura in cui, con atteggiamento pilatesco, sceglie di non affrontare il cuore del problema, vale a dire il tema dell'inquadramento giuridico delle *chat* criptate. Paradossalmente, esso viene affrontato attraverso una curiosa tecnica di ragionamento che resta in ipotesi: non conoscendo il contenuto del materiale digitale trasmesso nella sua interezza, i giudici hanno ritenuto di dover prendere in considerazione sia l'ipotesi ricostruttiva prospettata nell'ordinanza di rimessione sia quella difensiva, che qualificavano tali elementi, rispettivamente, come "documenti" ovvero come "dati di traffico".

---

[19] In proposito, volendo, cfr. L. MARAFIOTI, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento*, in T. BENE-L. LUPÁRIA DONATI-L. MARAFIOTI (a cura di), *L'ordine europeo di indagine. Criticità e prospettive*, Giappichelli, 2017, p. 9 ss.

Ad ogni modo, a parere della Corte, la soluzione rimane la medesima, nel senso che non sarebbe necessario alcun previo intervento da parte del giudice italiano.

Segnatamente, con riguardo alla prova documentale, sarebbe sufficiente un provvedimento del pubblico ministero per rispettare sia l'art. 15 Cost. sia l'art. 6, paragrafo 1, lett. *b),* Direttiva 2014/41/UE, ai sensi del quale l'autorità di emissione dell'ordine europeo d'indagine deve poter disporre l'atto di indagine richiesto alle stesse condizioni in una analoga vicenda interna.

Con riferimento ai dati di traffico, invece, la disciplina di cui all'art. 132 del D. Lgs. 30 giugno 2003, n. 196, nell'imporre la previa autorizzazione del giudice, disciplinerebbe la sola acquisizione dei dati presso il gestore dei servizi telefonici e telematici e non anche l'utilizzazione dei dati medesimi in un procedimento penale diverso. Per la loro circolazione, infatti, occorrerebbe fare riferimento alla disciplina generale di cui all'art. 238 c.p.p., bastando, cioè, il solo provvedimento del pubblico ministero.

In ultima battuta, le Sezioni Unite teorizzano il seguente assetto: a livello interno, il pubblico ministero può chiedere ed ottenere la disponibilità di prove già formate in un determinato procedimento penale, al fine di produrle in un altro procedimento, senza necessità di alcuna autorizzazione preventiva da parte del giudice competente per quest'ultimo. Ciò anche nel caso di prove, come le intercettazioni di conversazioni o di comunicazioni o l'acquisizione dei dati esterni di traffico, per la cui formazione è indispensabile la preventiva autorizzazione del giudice.

Ne consegue, quale corollario, che gli atti oggetto dell'ordine europeo d'indagine, costituenti prove già in possesso delle autorità competenti dello Stato di esecuzione possono essere legittimamente richiesti e acquisiti dal pubblico ministero italiano senza la necessità di preventiva autorizzazione da parte del giudice del procedimento nel quale si vorrebbe utilizzarli. Soltanto all'esito – vale a dire quando il pubblico ministero presenta al giudice le prove oggetto di acquisizione dall'estero – il giudice italiano "ricevente" deve controllare se vi fossero le condizioni per emettere l'ordine europeo d'indagine, così da assicurare il pertinente diritto di "impugnazione" nello Stato di emissione previsto dall'art. 14, paragrafo 2, della Direttiva.

Tuttavia, la soluzione appare, per così dire, piattamente "proceduristica" e si rivela, pertanto, inadeguata. Si preferisce, infatti, far leva esclusivamente sull'assetto interno in tema di circolazione probatoria per risolvere un delicato problema di cooperazione probatoria internazionale. Basti pensare al pericolo assai concreto che, attraverso l'emissione di un ordine europeo d'indagine, il pubblico ministero "deleghi" all'autorità estera lo svolgimento di attività probatoria per cui in Italia occorre il

provvedimento di un giudice, magari temendo che tali attività gli vengano negate o, peggio ancora, dopo che gli sono state negate.

Da questo angolo visuale, nascondersi dietro al meccanismo dell'ordine europeo d'indagine rappresenta una "scorciatoia" probatoria molto pericolosa, tanto più in un'epoca in cui si fa ampio uso di strumenti investigativi *ultra fines*. Si tratta, sostanzialmente, di congegni privi di una disciplina a livello codicistico interno e dall'elevatissimo tasso di invasività sulla sfera privata[20], come i captatori informatici "atipici". Si tratta di terreno dove il controllo sulla legittimità dell'uso di mezzi di ricerca della prova tecnologici è affidato al pendolo poco rassicurante della giurisprudenza[21].

A non convincere è, soprattutto, il modello di un controllo *ex post*, idealmente plasmato su una concezione di contraddittorio incentrato solo su una beffarda e apparente simmetria, frutto della riduzione a mera possibilità di "dire la propria" in un secondo momento, senza alcuno scrutinio sulla sua effettività. Invece di un controllo nel momento della formazione della prova, si slitta su quello successivo, in ordine all'assunzione e all'utilizzabilità della prova; un dibattito postumo di opinioni, per nulla aderente al modello di contraddittorio patrocinato dal codice di rito.

D'altra parte, la mera opportunità di contestare i risultati davanti al giudice italiano suona come un paradosso: può essere, infatti, impossibile contestare un dato che nessuno sa da dove provenga e come sia stato formato[22].

Né, al fine di pervenire ad approdi più rassicuranti, può essere apprezzato il richiamo, anch'esso contenuto nella pronuncia *de qua*, alla valenza rivestita dal principio del mutuo riconoscimento e dalla

---

[20] Cfr. F. CENTORAME, *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Riv. it. dir. proc. pen.*, 2021, p. 499 ss.

[21] *Ex multis*, per un approccio improntato alla deformalizzazione dell'attività investigativa digitale in materia di captatore informatico, v. Cass., Sez. I, 7 ottobre 2021, Romeo, in *Cass. pen.*, 2022, p. 3106 ss., con nota di A. PROCACCINO, *Piccoli equivoci senza importanza: tra intercettazioni di flussi informatici, perquisizioni e prove atipiche*; in *Giur. it.*, 2022, p. 2780 ss., con nota di L. ALGERI, *Lo* Screenshot *eseguito (senza garanzie?) dal* Trojan *di Stato*.

[22] È interessante notare che, nel sistema francese, il codice di rito prevede espressamente la possibilità di impiegare un «*dispositif technique ayant pour objet la captation de données informatiques*» e, a tal fine, può essere fatto ricorso a «*moyens de l'Etat soumis au secret de la défense nationale*» (Article 706-102-1). Tuttavia, al fine di consentire l'esercizio – sia pur minimo – di un contraddittorio tecnico, in quest'ultimo caso «*les résultats sont accompagnés des indications techniques utiles à la compréhension et à leur exploitation ainsi que d'une attestation visée par le responsable de l'organisme technique certifiant la sincérité des résultats transmis*» (Article 230-3). Proprio in tema di acquisizione di *chat* criptate, la *Cour de cassation* ha avuto modo di censurare l'assenza di un'attestazione tecnica che "certificasse" la genuinità delle operazioni compiute mediante dispostivi tecnici informatici: cfr. Cour de cassation, Chambre criminelle, 11 octobre 2022, 21-85.148, in www.legifrance.gouv.fr, nonché Cour de cassation, Chambre criminelle, 25 octobre 2022, 21-85.763, *ibidem*.

presunzione di conformità ai diritti fondamentali dell'attività svolta dall'autorità giudiziaria estera nell'ambito di rapporti di collaborazione probatoria[23].

In effetti, il richiamo a tali principi si risolve in un semplicistico dar per buone attività compiute nello Stato estero; cosicché, quella ventilata appare soluzione poco soddisfacente e scarsamente compatibile con gli artt. 24 e 111 Cost.

In definitiva, le Sezioni Unite si sono attestate su posizioni addirittura meno garantiste di quelle assunte di recente in materia dalla Corte di giustizia dell'Unione europea. In quella sede, si è avuto modo di chiarire che deve pur sempre sussistere la possibilità di un controllo giurisdizionale effettivo sul rispetto dei diritti fondamentali delle persone interessate[24]. I giudici europei hanno, infatti, ritenuto che l'art. 14 della Direttiva imponga al giudice penale nazionale di espungere, nell'ambito di un procedimento penale, informazioni ed elementi di prova se l'imputato non è in grado di svolgere *efficacemente* le proprie osservazioni su tali informazioni ed elementi di prova e questi ultimi siano idonei di influire in modo preponderante sulla valutazione dei fatti.

Di talché, il teorizzato atto di fede nell'operato della magistratura straniera mal si concilia, persino, con il *test* garantistico imposto dalla Corte di giustizia. Se, insomma, l'autorità giudiziaria straniera resta l'unico garante del rispetto delle forme attraverso le quali la prova può fare il suo ingresso nel processo "ricevente" è, allora, impossibile assicurare al giudice nazionale il suo ruolo di *gatekeeper* delle prove formate all'estero.

4. **Crittografia e contraddittorio in rotta di collisione**

L'aspetto ancor più criticabile della sentenza è, però, ancora un altro. Nella sentenza in commento, le Sezioni Unite affermano che l'impossibilità per la difesa di accedere all'algoritmo utilizzato per "decriptare" il contenuto dei dati digitali non determinerebbe alcuna violazione di diritti fondamentali[25].

---

[23] Cfr., nello stesso senso, Cass., Sez. I, 13 gennaio 2023, Costacurta, in *C.E.D. Cass.*, rv. 284440.

[24] Corte di Giustizia, Grande Sezione, sent. 30 aprile 2024, domanda pregiudiziale proposta dal *Landgericht Berlin* nel proc. M.N., causa C-670/22

[25] Nel medesimo senso, in giurisprudenza, già prima della pronuncia in commento, Cass., Sez. VI, 26 ottobre 2023, Rosaci, in *C.E.D. Cass.*, rv. 285494, secondo cui neppure il sistema di diritto interno garantirebbe alla difesa l'accesso agli algoritmi impiegati la decodifica dei dati criptati, limitandosi, per converso, a dettare garanzie procedurali finalizzate alla protezione della *chain of custody* e alla salvaguardia dell'integrità probatoria. V. anche Cass., Sez. VI, 11 ottobre 2023, Brunello, in www.italgiure.giustizia.it, nella quale i giudici candidamente affermano che «nell'ordinamento interno la conoscibilità delle

Ad escludere qualsiasi pericolo di alterazione dei dati sarebbe, infatti, la circostanza oggettiva che la decrittazione stessa è ormai avvenuta: poiché il contenuto di ciascun messaggio è inscindibilmente abbinato ad un'unica chiave di cifratura, l'utilizzo di una chiave errata avrebbe in caso condotto ad una omessa decrittazione e giammai ad una decrittazione errata[26].

Simile assunto ha indotto la Suprema Corte ad escludere qualsiasi violazione del diritto di difesa e della garanzia di un giusto processo, con conseguente piena utilizzabilità degli atti acquisiti mediante ordine europeo d'indagine.

Tuttavia, la piattaforma argomentativa delle Sezioni Unite per aggirare ogni questione in ordine alla violazione del diritto di difesa ed al contraddittorio lascia davvero perplessi. In realtà, non può seriamente dubitarsi che la mancata conoscenza delle tecniche di decodificazione del dato criptato crei per definizione un *vulnus* al diritto di difesa[27]. Molto semplicemente, non può esservi nessun controllo sulla prova tecnica perché non c'è alcun contraddittorio tecnico possibile.

A fronte di questo pacifico dato, le Sezioni Unite fanno irrompere sulla scena un singolare argomento, che potrebbe definirsi della "tirannia tecnica" ovvero "tecnologica". Vale a dire, incredibilmente: non sono tanto i principi ricavabili dalla legge e le garanzie riconosciute nel processo penale a dettare le modalità acquisitive o di utilizzo della prova. Piuttosto, è l'ineliminabile dimensione pratica del dato tecnico a condizionare e, in definitiva, pregiudicare irrimediabilmente la realtà della difesa, del contraddittorio e, in ultimo, del processo.

Non si tratta, peraltro, di un tema nuovo: sembra riecheggiare, addirittura, il dibattito del tempo intorno alla tortura, quando si escludeva, *faut de mieux*, che si potesse operare altrimenti per ricavare la verità.

---

eventuali tecniche di hackeraggio è […] preclusa dal "segreto industriale" del proprietario del *software* utilizzato per l'operazione di intrusione».

[26] L'assunto era già stato enunciato dalla Suprema Corte con riferimento alla decrittazione delle *chat* intercorse su sistemi *Blackberry*: cfr. Cass., Sez. IV, 21 aprile 2022, Chianchiano, in *C.E.D. Cass.*, rv. 283454.

[27] Nel senso del testo, in giurisprudenza, Cass., Sez. VI, 15 luglio 2022, Lori, in *Giur. pen.* web, 2023, n. 2, 6 febbraio 2023, con nota di A. BARBIERI, *I limiti di utilizzabilità dei messaggi crittografati scaricati da un server estero ed acquisiti mediante ordine europeo di indagine*. Nella pronuncia, i giudici di legittimità affermano con chiarezza che «la prova [trasmessa da autorità straniere] non può […] essere in contrasto con i principi fondamentali e inderogabili dell'ordinamento giuridico italiano e quindi con l'inviolabile diritto di difesa. E dunque lo scrutinio sulla compatibilità del processo di acquisizione del dato probatorio con il diritto di difesa è stato completamente frustrato dalla scelta della Procura di mettere a disposizione i soli esiti dell'attività svolta all'estero e non anche il percorso di acquisizione di quei dati, dovendosi anche sindacare l'idoneità, necessità e proporzionalità del dato probatorio nella prospettiva di garantire la minore lesione possibile dei diritti fondamentali».

Al di là di qualsiasi tecnicismo di stampo processualpenalistico su questo o quell'altro aspetto specifico della disciplina diventa, allora, indifferibile l'esigenza di più generale ripensamento della tematica, mediante un rinnovamento in senso, anzitutto, culturale, con l'avvento di un "nuovo illuminismo" in tema di prova, *a fortiori* qualora si tratti di prova "tecnica". Altrimenti, un processo basato sempre meno sulla prova orale rischia di essere quasi esclusivamente incentrato su dati "ricavati" attraverso strumenti tecnici senza garanzie adeguate.

Necessità che appare tanto più impellente se si pone mente alla prospettiva imminente di un processo pensato anche per l'intelligenza artificiale[28]. Anche in quest'ottica, un radicale mutamento di prospettiva in termini di esercizio del diritto di difesa e del contraddittorio appare doveroso[29]. A tale fine, però, non ci si deve limitare ad inseguire la tecnologia, restandone irrimediabilmente schiavi.

Viceversa, bisogna fare proprio il contrario: occorre, insomma, compiere più di un passo indietro rispetto alla pressione esercitata dall'ossessione tecnologica. Ricordare, cioè, che il tema della prova pur deve restare sempre sotto l'egida delle legalità, anziché sotto il tallone di ferro delle necessità della prassi, secondo l'unica prospettiva autenticamente compatibile con un'idea liberale di processo penale.

18.09.24

[28] Cfr. L. LUPÁRIA DONATI-G. FIORELLI, *Diritto probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale*, in *Dir. pen. proc. – Riv. trim.*, 2022, n. 2, p. 34 ss.
[29] Cfr. L. MARAFIOTI, *Intelligenza artificiale, giudizio penale e garanzie processuali*, in *Ind. Pen.*, 2023, p. 3 ss.