GIUSTIZIA INSIEME

Processo Penale

Sky ecc, ordine europeo di indagine tra giurisprudenza nostrana e comunitaria

di Francesco Agnino

10 dicembre 2024

Sommario: 1. Premessa: il quadro investigativo complesso dinnanzi alle Sezioni Unite. – 2. Le diverse soluzioni offerte dalla Corte di cassazione. – 3. Interrogativo pregiudiziale: raccolta massiva di dati o "captazione c.d. mirata". – 4. L'estensione della disciplina interna sulla circolazione delle prove fra procedimenti diversi. – 5. Nessun controllo giurisdizionale anticipato nello Stato di emissione. – 6. Il controllo giurisdizionale non è escluso (anche se postumo). – 7. Il controllo sulle ragioni di merito dell'emissione dell'OEI. – 8. Modalità di raccolta delle prove da parte dell'autorità straniera e controllo giurisdizionale. – 9. Nessuna critica?

1. Premessa: il quadro investigativo complesso dinnanzi alle Sezioni Unite

Le sezioni unite con le due sentenze gemelle nn. 23755 e 27356, depositate il 14 giugno 20124, hanno sciolto alcuni dubbi connessi al caso dei c.d. criptofonini *Sky ECC*.

Gli arresti nomofilattici devono essere letti congiuntamente alla decisione del 30 aprile 2024 con cui la Grande Sezione della Corte di giustizia dell'Unione Europea si è pronunciata in merito all'analoga vicenda dei messaggi criptati scambiati attraverso la piattaforma *Encrochat* (Corte giust., 30 aprile 2024, *M.N.*, C-670/22). E, comunque, un ulteriore tassello al mosaico verrà aggiunto dalla Corte europa dei diritti dell'uomo, anch'essa chiamata ad esprimersi al riguardo (procedimenti n. 44715/20 e 47930/21).

La diatriba, come è ormai ben noto, concerne la natura e le conseguenti garanzie procedimentali applicabili all'acquisizione delle conversazioni via *chat* intercorse fra alcuni esponenti di associazioni criminali dedite al traffico di stupefacenti attraverso piattaforme *online* di tipo criptato, che avevano loro consentito di comunicare in modo riservato mediante *smartphone* appositamente modificati.

Nell'esperire le attività istruttorie sui criptofonini, le forze di polizia francesi si sono avvalse di tecniche investigative particolarmente intrusive e articolate, tutt'ora parzialmente coperte da segreto di Stato, che hanno consentito di intercettare, acquisire e decodificare l'intera mole di comunicazioni convogliate su note piattaforme criptate come sky-ecc ed Encrochat (ma anche Ennetcom, PGP Safe, IronChat e ANOM).

Le operazioni hanno coinvolto chat individuali o di gruppo recanti milioni di messaggi riferibili a decine di migliaia di utenti dislocati in tutto il mondo. Per procedere alla captazione, i server e i criptofonini — nel caso sky-ecc basati su quattro diverse chiavi di cifratura — sono stati hackerati dalle autorità di contrasto francesi, operanti in una squadra investigativa congiunta (JIT – Joint Investigation Team) con le forze di polizia olandese e belga.

Gli esiti di tali attività istruttorie sono stati poi trasmessi, ricorrendo all'ordine europeo di indagine, agli organi investigativi degli Stati membri interessati.

La raccolta di dati in così grandi dimensioni ha sollevato complessi interrogativi concernenti la tutela della privacy, la validità delle prove digitali, la compatibilità con le regole del giusto processo sotto il versante della parità delle armi e la necessità di garantire l'inviolabilità del diritto di difesa. Per comprendere la rilevanza della questione, è sufficiente notare come le vicende sui criptofonini abbiano cagionato incidenti di costituzionalità, pronunce dei giudici interni di merito e di legittimità, oltre che l'intervento della Corte di giustizia dell'Unione europea: dalle corti francesi a quelle italiane, passando per le giurisdizioni belga, olandese, norvegese e tedesca, i tribunali del vecchio continente, di ogni ordine e grado, si sono trovati a dover fronteggiare i dilemmi che le operazioni istruttorie basate sui criptodati hanno originato

(ne dà conto la memoria per l'udienza delle sezioni unite penali del 29 febbraio 2024 della procura generale presso la Corte di cassazione, consultabile in , 1° marzo 2024, 83 s.: «il Conseil constitutionnel francese, con la decisione n. 2022-987 QPC dell'8 aprile 2022, ha statuito che la disciplina francese, sulla cui base eÌ stata disposta l'acquisizione delle chat e l'intercettazione delle comunicazioni operate nel presente procedimento, eÌ conforme alla Costituzione francese; il Bundesgerictshof, con la sentenza 5 StR 457/21 del 2 marzo 2022, ha ritenuto che l'intercettazione della piattaforma Encrochat, "violata" dall'autorità giudiziaria francese, fosse legittima ai sensi del diritto processuale penale tedesco; [...] la Corte suprema dei Paesi Bassi (Floge Raad), con la sentenza n. 913 del 13 giugno 2023, ha ritenuto conforme al diritto interno l'acquisizione dei dati informatici presenti sulle piattaforme criptate Encrochat e sky-ecc, acquisite dall'autorità giudiziaria francese").

Le Sezioni Unite, di conseguenza, si sono dovute confrontare con il tema dell'impiego dell'OEI ai fini della raccolta di prove già in possesso dell'autorità di esecuzione: un'eventualità espressamente prevista sia dalla direttiva sia dal d.lgs. n. 108 del 2017.

Innanzi al giudice della nomofilachia si è posto un problema di tenuta delle garanzie fondamentali e dai non trascurabili risvolti pratici, che, nel caso dell'Italia, si arricchisce anche dei più recenti moniti contenuti nell'ennesima pronuncia dell'affaire *Contrada* (Corte eur. diritti dell'uomo 23 maggio 2024, Contrada c. Italia (n. 4); sentenza, quest'ultima, che lascia trapelare un problema sistemico nell'ordinamento giuridico italiano: la legge processuale non offre sufficienti garanzie contro gli abusi nelle intercettazioni a carico di soggetti non direttamente coinvolti in un procedimento penale. E, infatti, uno dei rischi che si cela dietro l'acquisizione di un così ragguardevole volume di "corrispondenza" — stando agli ultimi insegnamenti della Corte costituzionale (Corte cost. 27 luglio 2023, n. 170, con cui il giudice delle leggi ha statuito che «il concetto di "corrispondenza" ricomprende ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza". La tutela accordata dall'art. 15 Cost. "si estende, quindi, ad ogni strumento che l'evoluzione tecnologica mette a disposizione a fini comunicativi, compresi quelli elettronici e informatici, ignoti al momento del varo della Carta costituzionale» (par. 4.2 del considerato in diritto). Secondo la Memoria per l'udienza delle sezioni unite penali del 29 febbraio 2024 della procura generale presso la Corte di cassazione, cit., 39: "[d]alle statuizioni della Corte costituzionale deriva che le chat acquisite dall'autorità giudiziaria francese debbano essere qualificate come corrispondenza") — è quello che l'operazione si traduca in una "battuta

di pesca" (c.d. f*ishing expedition*) con valenza meramente esplorativa. Esigenze, quelle che si stagliano all'orizzonte, che si mostrano allora tanto più impellenti quando si considerino le notizie che giungono ancora dalla Francia e che riguardano note e ben più in voga app di messaggistica crittografata (è il caso della nota app Telegram; per una ricostruzione v. La svolta di Telegram dopo l'arresto di Durov: consegnerà alle autorità indirizzi e numeri dei presunti criminali, v. La Repubblica, 24 settembre 2024).

2. Le diverse soluzioni offerte dalla Corte di cassazione

È emerso in giurisprudenza un rilevante contrasto interpretativo, sia in ordine alla individuazione dello strumento processuale "interno" da porre a parametro per l'importazione delle "chat" decrittate e richieste con gli OEI che al tipo e all'ambito del controllo giurisdizionale da svolgere nel nostro ordinamento in merito alla utilizzabilità dei dati probatori i raccolti all'estero. Secondo un orientamento giurisprudenziale, in tali casi non potrebbe farsi riferimento alla disciplina delle intercettazioni, poiché la stessa presuppone l'esistenza di flussi di comunicazioni in atto (in tal senso, Cass., sez. 6, 27 settembre 2023, n. 46482 che ha precisato "trattarsi di registrazioni di conversazioni già avvenute e, quindi, di dati "statici" assimilabili a corrispondenza, e non invece di intercettazioni). La fattispecie processuale potrebbe rientrare nella acquisizione di "corrispondenza informatica" (le "chat", già disponibili, appunto, nello Stato di esecuzione attraverso il precedente ricorso a mezzi di intercettazione). D'altronde, si aggiunge, l'art. 1, par. 1, della direttiva 2014/41 UE consente il ricorso all'OEI anche per l'acquisizione di prove che già sono in possesso delle competenti Autorità dello Stato di esecuzione e il successivo art. 13 della direttiva disciplina il "trasferimento delle prove" (comprese quelle "già in possesso dello Stato di esecuzione").

Secondo questa tesi, si tratterebbe, dunque, di atti probatori già nella disponibilità dell'Autorità giudiziaria francese, che li ha acquisiti con procedura conforme al proprio ordinamento. In questa ottica, si è affermato che, a tal fine, "il pubblico ministero può emettere l'ordine europeo di indagine con cui si richiede il trasferimento di dati documentali, in particolare di corrispondenza già acquisita in un procedimento penale nel paese membro di esecuzione, per il cui sequestro è ‹sufficiente, ai sensi dell'**art. 15 Cost.** e secondo le disposizioni interne, il provvedimento motivato del pubblico ministero, senza necessità di intervento del giudice per le indagini preliminari" (Cass., sez. 6, 27 settembre 2023, n. 46482, cit.).

Ove si ritenesse fondata tale opzione ermeneutica, la norma di riferimento dovrebbe dunque essere individuata in quella prevista dall'**art. 254-bis c.p.p.**, che consente appunto il sequestro di corrispondenza informatica. Pertanto, ove dovesse ritenersi accoglibile tale ricostruzione normativa, si renderebbe comunque necessaria una valutazione del Giudice cautelare in merito alla sussistenza, nel caso concreto, dei requisiti di necessaria proporzionalità e adeguatezza nel nostro sistema processuale.

V'è tuttavia da osservare che la richiesta di trascrizione, decodificazione o decrittazione delle comunicazioni intercettate, cui fa riferimento la richiamata disposizione dell'art. 43, comma 4, dovrebbe essere più correttamente interpretata come formulazione di un'istanza collegata ed accessoria a quella, principale, contenuta nell'ordine di indagine richiesto ad altre› Stato membro, al fine di intercettare una delle diverse forme di telecomunicazioni descritte nel primo comma dell'art. 43, come tali non già precedentemente acquisite nell'ordinamento richiesto, ma ancora da espletare e trasmettere, in via immediata (art. **43**, comma 3, lett. a) o successiva (art. **43** , comma 3, lett. b), in conseguenza della richiesta emessa in fase attiva dalle autorità italiane. Sotto altro, ma connesso profilo, una diversa prospettiva esegetica potrebbe essere più fondatamente seguita valorizzando il contenuto di ulteriori disposizioni del complesso micro-sistema normativo dell'ordine di indagine europeo. Dovrebbe però sempre valutarsi la legittimità della “trasposizione” dei risultati delle intercettazioni “aliene” alla luce della nostra disciplina processuale (ex **art. 270 c.p.p.** appunto) e, conseguentemente, l'utilizzabilità delle relative comunicazioni (G. Faillaci, *Le Sezioni Unite sull’acquisizione e l’utilizzabilità dei dati dei criptofonini importati a seguito di un ordine di indagine europeo. Nota a Corte di cassazione penale, sez. un., 14 giugno 2024, ud. 29 febbraio 2024, n. 23756*, in NJus).

In tale ottica, ferma restando la legittimità dell'attività di intercettazione delle comunicazioni svolta all'estero, ci si dovrebbe interrogare circa la possibilità, nel nostro ordinamento, di utilizzare il trojan, non solo per disporre un'intercettazione, ma anche per acquisire — attraverso il sistema sopra descritto – le chiavi di decrittaggio. 'aspetto relativo all'utilizzo del trojan per acquisire le chiavi di decrittaggio non risulta essere stato affrontato dalla giurisprudenza (i precedenti relativi ad intercettazioni effettuate su cellulari “blackberry”, di cui si darà conto infra, differiscono dalla situazione in esame perché per essi la socieietà gestrice forniva, su richiesta della Autorità giudiziaria, le comunicazioni decrittate). La Suprema Corte ha affermato il principio secondo cui le prove “atipiche” acquisite in violazione di un divieto derivante da principi costituzionali sono illecite e quindi inutilizzabili. Peraltro, ove si ritenesse che l'utilizzo del captatore informatico sia consentito, nel nostro ordinamento processuale, per effettuare “l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici

ovvero intercorrente tra più sistemi" (**art. 266 bis c.p.p.**), si potrebbe sostenere che l'attività di inoculazione del virus informatico, anche funzionale ad acquisire le chiavi di decrittaggio (trasmesse dai "criptofonini" a ciò indotti dal "malware"), si collochi comunque all'interno di una attività "intercettativa" di un flusso di comunicazioni informatiche. Va peraltro rilevato, al contempo, che tale conclusione non è affatto certa, atteso che l'utilizzo del captatore informatico è, nelle diverse disposizioni processuali previste dal codice di rito (artt. **266**, commi 2 e 2-bis, 267, commi 1 e 2-bis, 89 disp. att. c.p.p.), autorizzato soltanto per l'inserimento su un "dispositivo elettronico portatile". V'è altresì da considerare che, ai fini dell'impiego del captatore informatico, il nostro ordinamento, a seguito della recente interpolazione del testo dell'**art. 267, comma 1, c.p.p.** (intervenuta per effetto dell'**art. 1, comma 2-bis, D.L. 10 agosto 2023, n. 105**, convertito nella **legge 9 ottobre 2023, n. 137**), impone all'autorità giudiziaria l'assolvimento di un rigoroso onere motivazionale non solo nella indicazione delle specifiche ragioni che ne giustificano l'attivazione, ma anche nella esposizione di una autonoma valutazione della necessità, "in concreto", del ricorso a tale peculiare modalità tecnica di espletamento del relativo mezzo di ricerca della prova. Una motivazione, dunque, "rafforzata", attraverso la quale il Giudice è chiamato, nel rispetto del canone di proporzionalità, a spiegare le ragioni poste a fondamento dell'utilizzo di uno strumento di indagine particolarmente invasivo della riservatezza delle persone, dando conto, in concreto, del bilanciamento da lui operato tra i diversi beni di rilievo costituzionale confliggenti nel caso di specie. Ove la tesi sopra indicata — secondo la quale è legittimo l'utilizzo del captatore informatico nel caso di specie – sia ritenuta condivisibile, deve poi rilevarsi come, nella medesima prospettiva, sia stata ritenuta "legittima, ove ricorrono i presupposti di legge per l'autorizzazione, la disposizione di un successivo decreto di intercettazione sul medesimo bersaglio o dispositivo elettronico già colpito da attività investigativa, giustificata dalla necessità di far ricorso, per ragioni d'indagine, allo strumento più pervasivo del "captatore informatico", configurandosi in tal caso un nuovo ed autonomo mezzo di ricerca della prova che non presenta interferenze con le intercettazioni telefoniche e/o ambientali già disposte con i mezzi ordinari di captazione" (Cass., sez. 5, 24 settembre 2020, n. 32426).

I suindicati profili problematici si correlano, infine, anche al tema dell'utilizzabilità a fini probatori degli atti compiuti dall'Autorità estera e importati nel nostro ordinamento a mezzo di OEI. Infatti, l'art. 36 D.L.vo cit. stabilisce al comma 1 che "Sono raccolti nel fascicolo per il dibattimento di cui all'**articolo 431 del codice di procedura penale**: a) i documenti acquisiti all'estero mediante ordine di indagine e i verbali degli atti non ripetibili assunti con le stesse modalità; b) i verbali degli atti, diversi da quelli previsti dalla lettera a), ‹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". Un secondo nucleo di profili problematici — avente anch'esso un significativo rilievo e correlato al tema della utilizzabilità delle prove "aliene" acquisite nel nostro ordinamento — concerne in particolare la necessità che la difesa possa disporre, ove Io richieda, dell'algoritmo per la decrittazione delle "chat" (algoritmo che, a quanto consta, nel caso in esame non è stato comunicato all'Autorità giudiziaria italiana che ha ricevuto solo le conversazioni già tradotte "in chiaro"). Sul punto, in riferimento alle intercettazioni effettuate su un dispositivo cellulare "Blackberry" è ravvisabile un contrasto nella giurisprudenza di legittimità, che è anche "rifluito" in alcune delle pronunce relative alle chat intercorse su "sky ecc". Secondo un orientamento, ove l'attività di messa in chiaro di messaggi criptati scambiati mediante sistema "Blackberry" sia svolta dal fornitore del servizio fuori dal contraddittorio, la difesa ha diritto di ottenere, oltre alla versione originale e criptata dei messaggi, anche le chiavi di sicurezza necessarie alla decriptazione, a pena di nullità ex **art. 178, lett. c), c.p.p.**, sanabile dall'istanza di giudizio di abbreviato; in particolare, sul punto si è rilevato che laddove alla difesa – non solo in sede cautelare, ma anche nel corso del giudizio di merito – fosse precluso di prendere cognizione dei flussi di comunicazioni informatiche o telematiche, nella loro versione originale ed integrale, e fosse ‹conseguentemente impedito l'esercizio di ogni potere di controllo, sussisterebbe una nullità di ordine generale a regime intermedio, derivante dalla 'violazione della disciplina diretta ad assicurare l'assistenza e la rappresentanza dell'imputato in una ipotesi in cui, tuttavia, non è obbligatoria la presenza del suo difensore. In senso contrario, un diverso orientamento ha invece ritenuto che, «in tema di intercettazione di comunicazioni telematiche, l'uso dell'algoritmo per la decriptazione della messaggistica con sistema "Blackberry" esclude la possibilità di alterazioni o manipolazioni dei testi captati, in quanto, secondo la scienza informatica, ne consente la fedele riproduzione, salvo l'allegazione di specifici e concreti elementi di segno contrario» (Cass., sez. 3, 21 aprile 2022, n. 30395) e che «il difensore delle parti ha diritto di accesso al dato trasmesso in via digitale costituito dalle sequenze alfanumeriche o simboliche rappresentative della comunicazione oggetto di captazione (c.d. stringhe) e dal risultato della decodificazione intellegibile di tali sequenze, in quanto elementi integranti "informazione" o "registrazione" delle conversazioni o comunicazioni ai sensi dell'**art. 268, comma 7, cod. proc. pen.**» (Cass., sez. 3, 10 aprile 2019, n. 38009). D'altra parte, poi, per quanto riguarda l'attendibilità della decodificazione, non solo, significativamente, l'operazione di decriptazione per l'autorità giudiziaria è effettuata dalla stessa azienda che garantisce l'ordinario e regolare svolgimento delle comunicazioni, e, quindi, la criptazione e decriptazione delle stesse, tra gli utenti dei dispositivi oggetto di intercettazione.

Va infatti rilevato che, come puntualmente osservato in una recente decisione, “in assenza dell'algoritmo necessario alla decriptazione, risulta – secondo la scienza informatica – impossibile avere a disposizione un testo intellegibile in lingua italiana difforme dal reale, potendosi, al più avere, se del caso, una sequenza alfanumerica o simbolica ("stringa") priva di alcun senso», sicché, salvo l'allegazione di specifici e concreti elementi di segno contrario, deve escludersi l'avvenuta manipolazione delle captazioni” (Cass., sez. 6, 27 novembre 2019, n. 14395).

3. Interrogativo pregiudiziale: raccolta massiva di dati o “captazione c.d. mirata”

Un problema preliminare che l’interprete è chiamato a risolvere è stabilire se le attività istruttorie avviate in Francia si traducano in operazioni di “bulk interception of data”, cioè di raccolta massiva di dati o se, diversamente opinando, si tratti di una “captazione c.d. mirata”.

La giurisprudenza della Corte Edu, da tempo impegnata a tracciare i confini di tutela del diritto alla vita privata e familiare, al domicilio e alla corrispondenza, ha affrontato in più occasioni la delicata questione della captazione massiva di dati, originariamente circoscritta all'intercettazione collettiva — c.d. “sorveglianza segreta” — di telefoni fissi (Corte eur. diritti dell'uomo 6 settembre 1978, Klass e al. c. Germania, in), poi progressivamente estesa ai telefoni cellulari Corte eur. diritti dell'uomo 29 giugno 2006, Weber e Saravia c. Germany, in ; 1° luglio 2008, Liberty e al. c. Regno unito, ibid.; 4 dicembre 2015, Roman Zakharov c. Russia, ibid.) e più di recente alle intercettazioni indiscriminate effettuate dai servizi di intelligence.

I giudici di Strasburgo sono giunti ad ammetterne la liceità “per indagare su alcuni reati gravi” (Corte eur. diritti dell'uomo, grande camera, 25 maggio 2021, Big Brother Watch e al. c. Regno unito, in , § 345; 25 maggio 2021, Centrum för Rättvisa c. Svezia, ibid., § 259.) a condizione, però, che vengano previste efficaci garanzie contro il rischio di abusi e di arbitrii nelle fasi di adozione della misura, della sua esecuzione e del controllo successivo.

Per saggiare se le operazioni sky-ecc ed Encrochat, condotte nell'ambito di diversi procedimenti penali, siano qualificabili come “bulk interception of data” e valutarne l'ammissibilità anzitutto rispetto all'art. 8 Cedu, è possibile prendere a parametro di riferimento le indicazioni che i giudici convenzionali hanno fornito nelle citate *Big Brother Watch c. Regno unito* e *Centrum för Rättvisa c. Svezia*; pronunce, queste ultime, nelle quali è stata vagliata la conformità di pratiche di sorveglianza di massa — implicanti la raccolta di dati, metadati e comunicazioni elettroniche

— con le garanzie previste dalla convenzione europea dei diritti dell'uomo.

In tanto un'intercettazione può dirsi “di massa” in quanto presenti le seguenti caratteristiche: *i*) le comunicazioni riguardino un gran numero di persone, molte delle quali non sono affatto di interesse per le autorità di intelligence; *ii*) la captazione massiva è generalmente diretta alle comunicazioni internazionali; *iii*) in molti casi, lo scopo dichiarato dell'intercettazione massiva è quello di monitorare le comunicazioni di persone al di fuori della giurisdizione territoriale dello Stato e, infine; *iv*) l'intercettazione sembra essere utilizzata ai fini della raccolta di informazioni di intelligence estere.

È opportuno sottolineare che l'intercettazione di massa compiuta dai servizi segreti è operazione diversa rispetto a quella esperita nel contesto di un procedimento penale (come nei casi più recenti di sky-ecc ed Encrochat) con scopi di repressione. Anzitutto, diverge lo scopo della raccolta dei dati: l'intelligence solitamente esegue la captazione indiscriminata con l'intento di raccogliere informazioni di servizi segreti stranieri o di individuare e indagare tempestivamente su attacchi informatici, controspionaggio e atti di terrorismo. Le attività in seno alla piattaforma sky-ecc hanno invece perseguito l'obiettivo di contrastare reati di criminalità organizzata dedita al traffico internazionale di stupefacenti.

In secondo luogo, l'intercettazione collettiva in un contesto di intelligence è generalmente diretta alle comunicazioni di persone o organizzazioni al di fuori della giurisdizione territoriale dello Stato. Nell'operazione sky-ecc, il traffico di rete è stato intercettato attraverso l'utilizzo di uno o più trojan horses inoculati su server specifici utilizzati da sky-ecc Globalpresso un unico fornitore di servizi Internet in Francia. Questa intercettazione è dunque “più mirata”.

E infatti, secondo gli organi giurisdizionali di molti Stati europei, le indagini condotte sui criptofonini nei casi sky-ecc ed Encrochat non costituirebbero un'ipotesi di ”bulk interception of data”. Ad esempio, il Tribunale distrettuale di Amsterdam (Corte distrettuale di Amsterdam 17 marzo 2022), chiamato a pronunciarsi sulla vicenda Encrochat,pur ritenendo che possa sussistere «a (potential) large infringement on privacy» — una (potenziale) grande violazione della privacy — ha statuito che non si tratti affatto di “bulk data”, nel senso di raccolta indifferenziata di dati, essendo le captazioni indirizzate a un target definito di persone — gli utenti Encrochat — additate di un sospetto specifico — che la piattaforma venisse impiegata interamente o prevalentemente da partecipanti alla criminalità organizzata per compiere reati.

Tuttavia, stando anche agli ultimi approdi giurisprudenziali, occorre prestare estrema attenzione all'automatismo in forza del quale, considerate le caratteristiche tecniche degli strumenti di

messaggistica, la piattaforma criptata possa essere utilizzata «esclusivamente» da membri dell'organizzazione criminale, senza alcuna considerazione in ordine al ruolo eventualmente rivestito dall'imputato, dato che siffatta presunzione si riverserebbe direttamente sulla *fairness* processuale, pregiudicando l'art. 6 Cedu sotto il profilo del diritto di difesa (V. Veronica, *Criptofonini e indagini digitali transfrontaliere su larga scala: un difficile equilibrio tra privacy, fairness processuale ed esigenze di repressione dei reati*, in Foro it., 2024, II, 566).

Ciononostante, la motivazione *de qua* ricorre anche nelle pronunce di altri tribunali olandesi (Corte distrettuale del North Holland 4 maggio 2022; Corte distrettuale del Zeeland-West-Brabant 10 giugno 2022), tra le motivazioni dei giudici di merito italiani (Trib. Reggio Calabria, ord. 29 agosto 2023: si tratta di apparecchi non intercettabili, progettati per le attività criminali e normalmente utilizzati — tenuto conto anche degli esorbitanti costi e della necessità di conoscere i nickname delle persone con cui si vuole conversare — da strutturate organizzazioni criminali), in alcune sentenze della Corte suprema norvegese (Corte suprema norvegese 30 giugno 2022, HR-2022-1314-A, case no. 22-027874STR-HRET, case no. 22-027879STR-HRET e case no. 22-027883STR-HRET) e della Corte suprema federale tedesca (Bundesgerichtshof tedesco, sent. 5 StR 457/21 del 2 marzo 2022); decisioni, queste, in cui è stata stabilita in modo definitivo la legittimità dell'uso dei dati di Encrochat e sky-ecc nei procedimenti penali (per la Francia, Conseil constitutionnel, decisione n. 2022-987 QPC, dell'8 luglio 2022; per la Germania, Bundesgerichtshof, sent. 5 StR 457/21 del 2 marzo 2022, cit.; per i Paesi Bassi, Hoge Raad, sent. 913 del 13 giugno 2023).

Le operazioni di captazione di grandi quantità di dati, in blocco o meno, si articolano in un *iter* procedurale ben preciso: *a*) l'intercettazione e la conservazione iniziale delle comunicazioni e dei dati relativi alle comunicazioni (cioè i dati di traffico appartenenti alle comunicazioni intercettate); *b*) l'applicazione di “selettori specifici” al materiale raccolto; *c*) l'analisi per estrarne informazioni rilevanti e, infine, *d*) la successiva conservazione dei dati e il loro impiego, che include eventualmente anche la condivisione con terzi. I giudici convenzionali ritengono che l'art. 8 Cedu proietti la sua tutela lungo ciascun segmento, sebbene l'interferenza sia progressivamente tanto più marcata quanto più avanzata è la fase in cui stazioni l'operazione.

Tra le garanzie che la Corte Edu ritiene necessarie in operazioni che involgono una grande quantità di dati spicca, senza dubbio, il controllo che un'autorità indipendente è chiamata a esercitare su ciascuna fase, in modo tale che l'ingerenza sui diritti umani possa essere limitata a ciò che è “necessario in una società democratica”.

In particolare, l'organo di controllo dovrebbe valutare la necessità e la proporzionalità dell'azione intrapresa, tenendo debitamente conto del corrispondente livello di intrusione nei

diritti tutelati dalla convenzione.

Al riguardo dirimente è la presenza di «garanzie end-to-end»: al fine di ridurre al minimo il rischio di abuso, la corte considera che, a livello nazionale, deve essere effettuata una valutazione in ogni fase del processo circa la necessità e la proporzionalità delle misure adottate; che l'intercettazione di massa debba essere soggetta a autorizzazione indipendente all'inizio, quando vengono definiti l'oggetto e l'ambito dell'operazione; e che l'operazione debba essere soggetta a supervisione e revisione indipendente *ex post facto*.

Secondo la corte, queste sono salvaguardie fondamentali di qualsiasi regime di intercettazione di massa conforme all'art. 8 Cedu. È altamente probabile che, a prescindere dalla circostanza che si tratti di “bulk data” o meno, analoghe garanzie verranno richieste anche nei casi sky-ecc ed Encrochat.

Nella prima fase — quella che potremmo definire di “raccolta” — le autorità francesi hanno ottenuto un'autorizzazione per intercettare i dati per un periodo di tempo limitato e per trasferirli ad altri Stati al fine di trovare una soluzione per decifrare il traffico di rete. Una tecnica di decriptazione, sviluppata dalle autorità olandesi (c.d. “sistema Hansken”), è stata poi condivisa con la polizia francese. Un giudice d'oltralpe ha quindi successivamente autorizzato l'intercettazione per un periodo di tempo più lungo. In sintesi, un test sulla necessità e la proporzionalità si è svolto nella fase di raccolta dell'operazione sky-ecc.

Le attività compiute in Francia debbono essere considerate legittime sulla base del principio di fiducia reciproca: tra gli Stati membri dell'Unione non sussistono regole uguali per l'assunzione della prova; si suppone, invece, un analogo livello di protezione dei diritti individuali. Quando emette un o.e.i. diretto al trasferimento di prove esistenti, l'autorità di emissione è vincolata al principio del mutuo riconoscimento, che costituisce la “pietra angolare” su cui si fonda la cooperazione in materia penale nell'Unione europea. Poiché i dati di Encrochat e sky-ecc sono stati intercettati dalle autorità francesi nell'ambito di un'indagine condotta sulla base del loro codice di procedura penale, il ricorso al principio della mutual trust implica che gli organi giurisdizionali chiamati a valutare gli esiti delle attività istruttorie condotte in Francia, debbono ritenere affidabili e legittime le intercettazioni dei dati.

La circostanza che la prima delle quattro fasi, quella di raccolta, sia stata assistita dalle garanzie procedurali necessarie assicura la legittimità delle attività istruttorie francesi sul versante dell'art. 8 Cedu. Resta, quindi, da determinare se le operazioni compiute — tanto in Francia,

quanto in Italia dopo la trasmigrazione dei dati e ancora coperte da segreto di Stato — siano state condotte in maniera tale da rispettare i diritti sanciti, nell'alveo del giusto processo, dall'art. 6 Cedu. Fatta salva la necessità del relativo bilanciamento con interessi quali la sicurezza nazionale o la segretezza dei metodi di indagine della polizia, infatti, occorre verificare se gli atti istruttori richiesti siano stati acquisiti nel rispetto delle garanzie procedimentali che, anche alla luce del diritto interno (art. 268, commi 6, 7 e 8, c.p.p.), obbligano a mettere la difesa nelle condizioni di conoscere le modalità di acquisizione delle comunicazioni scambiate mediante il sistema sky-ecc, per verificare la corrispondenza dei testi acquisiti in originale e dei testi decodificati, nonché la coincidenza delle utenze dei soggetti identificati come mittenti e destinatari (V. Veronuca, *Criptofonini e indagini digitali transfrontaliere su larga scala: un difficile equilibrio tra privacy, fairness processuale ed esigenze di repressione dei reati*, cit.).

4. L’estensione della disciplina interna sulla circolazione delle prove fra procedimenti diversi

Le Sezioni Unite si sono occupate preliminarmente di individuare la natura delle operazioni istruttorie in questione, le quali non consistono in un’acquisizione di documenti e dati informatici conservati all’estero” ai sensi dell’art. 234 *bis* c.p.p. (M. Daniele, ***Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/Encrochat in attesa delle Sezioni Unite***, in *sistemapenale.it*, 11 dicembre 2023; E. Lorenzetto, *L’acquisizione all’estero di comunicazioni digitali criptate nella fucina dell’ordine europeo di indagine penale*, in *Cass. pen.*, 2024, p. 182 s.).

Quest’ultima, osserva la Corte di cassazione, è una disciplina “alternativa e incompatibile” rispetto a quella dettata in tema di OEI; essa “prescinde” “da forme di collaborazione con l’autorità giudiziaria di altro Stato”, laddove il *Considerando* 35 della direttiva qualifica l’OEI come prevalente su tutti gli altri pertinenti strumenti internazionali che dovessero concorrere in materia.

Nel caso dell’OEI operano le garanzie che devono assistere la raccolta delle prove tramite questo strumento. In particolare, il principio di equivalenza, ai sensi di cui l’atto di indagine richiesto nell’OEI dovrebbe poter essere emesso “alle stesse condizioni in un caso interno analogo”; e il principio di proporzionalità, il quale esige che le eventuali compressioni dei diritti fondamentali originate dalle attività istruttorie siano contenute nello stretto necessario, e comunque non

intacchino i nuclei essenziali dei medesimi.

Il problema, qui, è comprendere come tali principi operino rispetto a prove che, in quanto autonomamente raccolte dalle autorità straniere, sono già state preformate sulla base della *lex loci*, a prescindere dalle regole previste dalla *lex fori*.

Siccome la direttiva e il d.lgs. n. 108 del 2017 si disinteressano della questione, non resta che prendere le mosse dall'art. 78 disp. att. c.p.p., relativo all'acquisizione della "documentazione di atti di un procedimento penale compiuti da autorità giudiziaria straniera": una prescrizione concepita in un momento storico in cui l'unico strumento di raccolta transnazionale delle prove era rappresentato dalle rogatorie, ma che può senz'altro essere ritenuta applicabile anche all'OEI. (M. Daniele, *Le sentenze gemelle delle Sezioni Unite sui criptofonini*, in www.sistemapenale.it).

Vi si prevede, al comma 1, che la documentazione in questione "può essere acquisita" nei procedimenti penali nazionali "a norma dell'articolo 238 del codice": vale a dire, delle prescrizioni che, in ambito nazionale, regolano la circolazione delle prove da un procedimento penale ad un altro.

Per le Sezioni Unite, venendo in gioco prove già autonomamente raccolte dalle autorità straniere prima dell'emissione dell'OEI, l'equivalenza con in casi interni analoghi va parametrata in rapporto non alla disciplina nazionale della "formazione", ma a quella della "circolazione" delle prove fra procedimenti diversi.

Da tale premessa, ne discende quale corollario che in questi casi le sole regole probatorie rilevanti ai fini dell'acquisizione in Italia delle prove già raccolte all'estero sono quelle rinvenibili nell'art. 238 c.p.p., a cui l'art. 78 disp. att. rinvia; nonchè, qualora le prove fossero state acquisite con le forme delle intercettazioni di comunicazioni, quelle rinvenibili nell'art. 270 c.p.p., il quale, sebbene non espressamente richiamato, può ritenersi applicabile in virtù della logica sottesa all'art. 78 disp. att.

5. Nessun controllo giurisdizionale anticipato nello Stato di emissione.

Inoltre, per il giudice di legittimità deve escludersi che per l'emissione di un OEI finalizzato all'acquisizione di comunicazioni criptate già autonomamente raccolte all'estero, sia necessaria

l'autorizzazione preventiva di un giudice dello Stato di emissione.

Se la circolazione di prove del genere da un procedimento ad un altro avvenisse a livello nazionale, tale autorizzazione preventiva non servirebbe, in quanto non richiesta nè dall'art. 238, nè dall'art. 270 c.p.p.

In applicazione del principio di equivalenza, pertanto, la Corte di cassazione ritiene che pure il corrispondente OEI possa essere emesso direttamente da un pubblico ministero. Ciò, si badi bene, anche quando le prove richieste fossero già state raccolte all'estero attraverso intercettazioni o acquisizione di tabulati: vale a dire, operazioni istruttorie che, a differenza delle perquisizioni e dei sequestri, a livello nazionale non potrebbero essere disposte direttamente dal pubblico ministero, ma necessiterebbero di una preventiva autorizzazione giurisdizionale.

Tale conclusione trova una conferma anche nella più sopra menzionata sentenza della Corte di giustizia relativa al caso *Encrochat*.

Il pubblico ministero, osservano i giudici di Lussemburgo, figura tra i soggetti che, ai sensi dell'art. 2 lett. *c* della direttiva, possono costituire un'autorità di emissione dell'OEI. L'unica condizione è che l'organo di accusa sia competente, in un caso interno analogo, "ad ordinare un atto di indagine diretto alla trasmissione di prove già in possesso delle autorità nazionali competenti".

6. Il controllo giurisdizionale non è escluso (anche se postumo)

Sotto il profilo della garanzia del diritto costituzionale della libertà personale, la Corte di cassazione non esclude che nello Stato emissione sia possibile prescindere da un vaglio giurisdizionale *tout court*.

Ciò discende dal già ricordato obbligo di rispettare i diritti fondamentali nei limiti del principio di proporzionalità, rispetto a cui il controllo giurisdizionale rappresenta un prerequisito essenziale.

Neppure va trascurata l'esigenza di assicurare che agli atti istruttori richiesti nell'OEI siano applicabili "mezzi d'impugnazione equivalenti a quelli disponibili in un caso interno analogo", tali da permettere, nell'ambito dello Stato di emissione, di contestare le "ragioni di merito dell'emissione dell'OEI".

Inoltre, lo Stato di emissione dovrebbe assicurare un mezzo di impugnazione nei confronti dell'OEI perfino quando questo non fosse contemplato in rapporto ad un caso interno analogo: un dovere non statuito dalla direttiva, ma introdotto dalla sentenza *Gavanozov II* della Corte di giustizia dell'Unione Europea in applicazione del diritto ad un ricorso effettivo previsto dall'art. 47 della Carta dei diritti fondamentali dell'Unione Europea (c.d. Carta di Nizza), al fine di assicurare uno *standard* di tutela unitario indipendente dalle caratteristiche degli ordinamenti dei singoli Stati (Corte giust., 11 novembre 2021, *Gavanozov II*, C-852/19).

Il giudice della nomofilachia ritiene di attribuire tale vaglio al giudice nazionale chiamato ad utilizzare le prove autonomamente raccolte all'estero e trasmesse tramite l'OEI: in particolare, al giudice di merito o al giudice chiamato ad applicare una misura cautelare, i quali conservano "integro il potere di valutare se vi siano i presupposti" per "ammettere" ed "utilizzare" tali prove ai fini delle decisioni di loro spettanza".

A tale soluzione si potrebbe contestare che così non si garantirebbe il diritto al controllo giurisdizionale attraverso un mezzo specifico di impugnazione, postulato dalla sentenza di *Gavanozov II* della Corte di giustizia a prescindere dalla sua previsione da parte dell'ordinamento dello Stato di emissione in un caso interno analogo, ma è stato efficacemente sottolineato in dottrina che tale diritto, in quella sentenza, non è identificato in modo così netto. Per quanto, infatti, la Corte di giustizia richieda che le persone coinvolte dagli atti istruttori disposti con l'OEI dispongano di "mezzi di impugnazione appropriati", essa comunque non esclude che si possa equiparare a questi ultimi il vaglio di ammissibilità operato dal giudice dello Stato di emissione chiamato ad utilizzare le prove (M. Daniele, *Le sentenze gemelle delle Sezioni Unite sui criptofonini*, cit.).

Ne consegue che il controllo giurisdizionale *ex post* esercitato dal giudice deputato ad utilizzare le prove già autonomamente raccolte all'estero può risultare sufficiente.

Il vero problema, piuttosto, riguarda i limiti di tale controllo.

L'art. 14 § 7 della direttiva si limita a richiedere il rispetto dei "diritti della difesa" e delle "garanzie del giusto processo nel valutare le prove acquisite tramite l'OEI".

A livello nazionale, non è molto più preciso l'art. 36 del d.lgs. n. 108 del 2017, che ripropone la medesima regola prevista dall'art. 431 comma 1 lett. *d* c.p.p. per l'utilizzabilità delle prove raccolte tramite le rogatorie: sono ammissibili 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".

La laconicità dei testi normativi comporta il rischio di sfumare i contorni del controllo esercitato dal giudice chiamato ad utilizzare le prove.

Le sentenze in commento precisa che ai fini dell'utilizzabilità nello Stato di emissione di atti acquisiti mediante OEI, "è necessario garantire il rispetto dei diritti fondamentali previsti dalla Costituzione e dalla Carta dei diritti fondamentali dell'Unione Europea, e, tra questi, del diritto di difesa e della garanzia di un giusto processo"; "ma non anche l'osservanza, da parte dello Stato di esecuzione, di tutte le disposizioni previste dall'ordinamento giuridico italiano in tema di formazione ed acquisizione di tali atti", considerato che nessuna norma della direttiva e del d.lgs. n. 108 del 2017 "prevedono, 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".

Dalla lettura dell'ordito motivazionale sembra che le Sezioni Unite individuano almeno due specifici requisiti di utilizzabilità.

Anzitutto, quando vengano in gioco prove raccolte autonomamente all'estero tramite atti che, come le intercettazioni o l'acquisizione di tabulati, a livello nazionale richiederebbero l'autorizzazione preventiva di un giudice, la Corte di cassazione pare richiedere una condizione ben precisa: il fatto che l'acquisizione delle suddette prove fosse a suo tempo stata autorizzata *ex ante* da un giudice nello Stato di esecuzione.

Tale presupposto, perlomeno nel caso esaminato dalla sentenza *Giorgi*, poteva ritenersi integrato, se si considera che le comunicazioni criptate erano state acquisite a seguito di provvedimenti motivati emessi da *juges d'instruction* francesi.

In secondo luogo, la sentenza *Giorgi* aggiunge che, qualora le comunicazioni fossero state autonomamente acquisite all'estero con la forma delle intercettazioni, sarebbe necessaria la loro rilevanza per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza, così come previsto dall'art. 270, comma 1, c.p.p.

Qualora, poi, tali intercettazioni fossero state eseguite all'estero in rapporto ad indirizzi di comunicazione situati in Italia, opererebbe senz'altro l'obbligo di notifica delle operazioni alle competenti autorità italiane in forza degli artt. 31 della direttiva e 24 del d.lgs. n. 108 del 2017. In questi casi, le intercettazioni diverrebbero inutilizzabili qualora non fossero ammissibili in un caso interno analogo: vale a dire, per quanto concerne l'Italia, se fossero state disposte in rapporto a reati per i quali non sarebbero consentite secondo l'ordinamento interno.

Inoltre, “l’onere di allegare e provare i fatti da cui inferire la violazione di diritti fondamentali grava sulla difesa, quando è questa a dedurre l’inutilizzabilità o l’invalidità di atti istruttori acquisiti dall’autorità giudiziaria italiana mediante OEI”: un principio, quest’ultimo, anch’esso operante nel settore delle rogatorie (Cass., Sez. 2, 18 maggio 2010, n. 24776), e comunque in linea con quanto avviene a livello nazionale, laddove spetta a chi afferma l’esistenza di un’invalidità processuale addurre i fatti che ne sono a fondamento.

Considerazioni non molto diverse sono, del resto, rinvenibili nella sentenza *Encrochat* della Corte di giustizia, laddove si legge che l’autorità di emissione, quando intenda ottenere la trasmissione di prove già in possesso delle competenti autorità dello Stato di esecuzione, “non è autorizzata a 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 di condurre ad un “sistema più complesso e meno efficace”, in violazione dei principi del mutuo riconoscimento e della fiducia reciproca che connotano il sistema della cooperazione giudiziaria nell’ambito dell’Unione Europea.

7. Il controllo sulle ragioni di merito dell’emissione dell’OEI

Al contrario, il controllo operato dal giudice nazionale chiamato ad utilizzare le prove, anche se già autonomamente raccolte all’estero, non può prescindere da un vaglio del rispetto dei presupposti di merito di emissione dell’OEI stabiliti dalla *lex fori*.

Si tratta di un controllo che, specie laddove la *lex loci* non fosse contraddistinta da adeguati *standard* di garanzia, costituisce un passaggio indispensabile per assicurare che le attività istruttorie, nel comprimere i diritti fondamentali e, in particolare, la garanzia di riservatezza (artt. 8 CEDU e 7 Carta di Nizza) di cui godono le comunicazioni di cui di discute, rispettino il principio di proporzionalità.

In particolare, laddove le operazioni istruttorie fossero avvenute all’estero con le forme delle intercettazioni o dell’acquisizione di tabulati, tale vaglio, sia pure nel rispetto dell’onere di allegazione a carico di chi proponga eventuali contestazioni, non potrebbe trascurare i requisiti la cui inosservanza, a livello nazionale, determinerebbe l’inutilizzabilità delle prove raccolte: si pensi alla presenza di indizi dei reati elencati dal codice e, per quanto concerne le intercettazioni, all’assoluta indispensabilità.

Qualche accenno in questo senso è, peraltro, rinvenibile nella decisione *Encrochat* della Corte di giustizia, laddove si afferma che "il carattere necessario e proporzionato" dell'emissione dell'OEI deve essere "valutato unicamente" alla luce del diritto dello Stato di emissione, e si ribadisce la necessità di evitare che l'impiego dell'OEI ai fini della trasmissione di prove già autonomamente raccolte all'estero abbia l'effetto di eludere le condizioni previste dalla *lex fori*.

"Di conseguenza", concludono i giudici di Lussemburgo, "se l'acquisizione di prove già in possesso delle autorità competenti di un altro Stato membro 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 ricorso contro l'ordine europeo di indagine che dispone tale trasmissione dovrebbe trarne le conseguenze che si impongono in base al diritto nazionale". Ossia, verrebbe da dire, dovrebbe applicare i divieti probatori che, a parità di condizioni, opererebbero in casi interni analoghi.

8. Modalità di raccolta delle prove da parte dell'autorità straniera e controllo giurisdizionale

Il controllo operato dal giudice nazionale chiamato ad utilizzare le prove, sempre in osservanza dell'onere di allegazione a carico di chi eccepisca una violazione, deve riguardare anche le modalità con cui esse sono state raccolte all'estero, specie laddove queste fossero tali, in ambito nazionale, da originare un divieto probatorio.

Qui viene in gioco un problema connesso alla peculiare natura delle operazioni istruttorie di cui si discute, le quali consistono in sofisticate attività di acquisizione e di decriptazione da svolgere attraverso idonee tecniche informatiche e specifici algoritmi. Il pericolo, se non vengano compiute in modo corretto, è che diano origine ad esiti falsati, e non siano quindi in grado di rappresentare fedelmente il contenuto delle comunicazioni.

Al fine di scongiurare questo rischio, l'ideale sarebbe che la difesa della persona sotto procedimento potesse venire a conoscenza delle modalità di acquisizione delle comunicazioni e, in particolare, degli algoritmi utilizzati per decriptarle. In questo modo, anche attraverso la nomina di consulenti tecnici di parte, si realizzerebbe un pieno contraddittorio di tipo tecnico, prezioso per la corretta valutazione del peso probatorio delle comunicazioni acquisite (M.

Daniele, *Le sentenze gemelle delle Sezioni Unite sui criptofonini*, in www.sistemapenale.it).

Il problema, tuttavia, è che spesso la trasmissione di tali informazioni da parte delle autorità straniere non avviene: vuoi per esigenze di segretezza dei metodi di indagine impiegati, al fine di non consentire agli esponenti della criminalità di prendere contromisure volte a nascondere le proprie comunicazioni attraverso tecniche informatiche ancora più efficaci; vuoi, addirittura, per esigenze di sicurezza nazionale, magari tali da giustificare l'apposizione del segreto di Stato.

In casi del genere, non ne deriverebbe l'inutilizzabilità delle prove: tale esito non si verificherebbe neppure a livello nazionale, non essendo rinvenibile nel nostro sistema un divieto probatorio volto a sanzionare questo tipo di situazioni. È chiaro, tuttavia, che il contraddittorio ne risulterebbe depotenziato, potendo conseguirne una distorsione dell'accertamento dei fatti.

Ed è essenziale che il giudice chiamato ad utilizzare le prove ne sia ben consapevole, in modo tale da andare alla ricerca di adeguati elementi di riscontro alle prove così ottenute.

Le Sezioni Unite affermano che l'impossibilità per la difesa di conoscere gli algoritmi utilizzati dall'autorità giudiziaria straniera per la decriptazione delle comunicazioni "non determina, almeno in linea di principio, una violazione di diritti fondamentali". Se è vero, ammette la Corte di cassazione, che la disponibilità di tale algoritmo è "funzionale al controllo di affidabilità del contenuto delle comunicazioni", deve però osservarsi che "il pericolo di alterazione dei dati non sussiste, salvo specifiche allegazioni di segno contrario, in quanto il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, per cui una chiave errata non ha alcuna possibilità di decriptarlo, anche solo parzialmente".

9. Nessuna critica?

Le due sentenze delle sezioni unite lasciano aperti molteplici interrogativi in ordine alla mancata conoscenza dei contenuti digitali, alla conseguente impossibilità delle difese di contrastarne gli esiti nonché da ultimo in relazione alla sufficienza del controllo giurisdizionale *ex post* rispetto ai gravi *vulnera* arrecati alla difesa.

L'assunzione a parametro "d'importazione" dell'art. 270 c.p.p., stando a quanto stabilito dai commi 2 e 3 della disposizione, dovrebbe garantire anche nella vicenda *ad quem* l'accesso diretto alla fonte di prova; accesso diretto che è stato reputato dalla Corte costituzionale (Corte cost. 10 ottobre 2008, n. 336) presupposto indefettibile per valutare la genuinità della prova e per verificare l'effettiva valenza dimostrativa degli elementi probatori. Ove il dato grezzo — che

dovrebbe essere depositato unitamente a tutti i metadati — sia criptato, sarebbe necessario mettere a disposizione delle parti e del giudice la chiave per decifrarlo. Nella medesima direzione si muove peraltro l'art. 14, par. 7, della direttiva sull'ordine europeo di indagine, che nell'interpretazione offerta dalla Corte di giustizia (Corte giust. 30 aprile 2024, causa C-670/22, M.N., cit.) impone di espungere dal procedimento informazioni ed elementi di prova idonei ad influire in modo preponderante sulla valutazione dei fatti se l'imputato non sia in grado di svolgere efficacemente le proprie osservazioni.

L'approdo dei giudici di Lussemburgo parrebbe andare ben oltre le conseguenze della nullità a regime intermedio argomentabile dalla disciplina dell'intercettazione in caso di violazione delle disposizioni procedurali, per giungere sino ad affermare una vera e propria regola generale di inutilizzabilità patologica.

Secondo il costrutto delle sezioni unite, invece, l'asserita infallibilità dell'algoritmo — cui segue una fideistica presunzione di integrità dei dati trasmessi dall'autorità straniera — renderebbe del tutto superflua ogni garanzia difensiva di accesso, minando in radice il diritto di difesa (V. Veronica, *Criptofonini e indagini digitali transfrontaliere su larga scala: un difficile equilibrio tra privacy, fairness processuale ed esigenze di repressione dei reati*, cit. che evidenzia che l'impiego crossborder della prova allogena digitale acquisita su larga scala con mezzi tecnologici invasivi e decriptata fuori dal contraddittorio è elemento conoscitivo a tal punto seduttivo da divenire centro di gravità fagocitante le garanzie processuali: presunzioni di legittimità, di integrità, di genuinità e di affidabilità — disinvoltamente affermate dalle sezioni unite — evocano il sospetto, più che giustificato, che difficilmente le soluzioni delle sentenze in rassegna, sotto il versante del diritto di difesa e della parità delle armi, resisterebbero al giudizio incisivo della Corte europea dei diritti dell'uomo).