L'utilizzo delle comunicazioni criptate da parte della criminalità organizzata

– di Giuseppina Laura Candito Giudice per le indagini preliminari del Tribunale di Reggio Calabria

L'evoluzione tecnologica non ha lasciato indifferente la vita delle organizzazioni criminali che precorrendo i tempi e rendendosene comunque protagoniste hanno ben compreso che **il digitale costituisce certamente una nuova frontiere per potenziare il loro *business*.**

La **rete** spazio non fisico, di per sé più difficilmente perimetrabile, controllabile e aggredibile, **diventa, quindi, da una parte luogo in cui commettere reati e dall'altra mezzo per le comunicazioni che ne consentono l'organizzazione**. All'interno di quello che in gergo viene definito ***dark web*** vengono acquistate armi e esplosivi, viene alimentato e gestito il narcotraffico, avviene la propaganda, l'indottrinamento, il finanziamento di atti terroristici, vengono diffuse e scambiate anche immagini a contenuto pedopornografico.

In questo senso, **l'attualità restituisce due costanti l'utilizzo di criptofonini e di piattaforme criptate o di chat segrete.** Se, dunque, il lessema comune a questi due poli sta nella radice "***cripto***" si evince come nella conduzione delle indagini "***decifrare***" sia uno tra gli obiettivi che si impone agli operatori del diritto.

Difronte alla sofisticazione dei meccanismi di comunicazione tesi sempre di più all'occultamento e all'elusione, dematerializzati e privi di confini, la principale risposta investigativa **che funge da contraltare si rinviene nel ricorso alla cooperazione internazionale** e **nel potenziamento della circolazione degli atti investigativi tra procedimenti transfrontalieri attraverso le JIT, gli OIE e le rogatorie.**

Al di là del *nomen* di questi strumenti i principi di fondo che ne regolano il funzionamento sono quelli di mutuo riconoscimento e di reciproco affidamento sul rispetto dei diritti fondamentali. **Così come le mafie travalicano sempre più i confini nazionali, anche le indagini e gli sforzi delle Procure così come i vagli che competono ai G.I.P. coinvolgono spesso più Stati, più forze di Polizia e più Autorità Giudiziarie.**

Procedendo per gradi, deve premettersi che **i criptofonini** sono accomunati dalle garanzie di anonimato e riservatezza dei contenuti comunicativi. Tali obiettivi sono resi possibili attraverso **accorgimenti nella fase dell'acquisto e puntuali modifiche sull'*hardware* e sul *software:***

- nessuna correlazione immediata tra account del cliente e il dispositivo o una sim card,
- acquisti da speciali rivenditori che non possiedono un punto vendita fisico e che si servono di canali occulti,
- elevato prezzo da pagarsi in contanti o in criptovalute pressoché pari ad un importo non inferiore a 1.600,00 euro,
- sistema operativo con interfaccia criptata, rimozione della telecamera, del microfono, del GPS, della porta USB funzionante solo ai fini del ricarico energetico, autodistruzione dei messaggi scambiati tra gli utenti, meccanismi di alterazione della voce, disattivazione del Bluetooth, l'impiego di Fake App, la possibilità di rilevare

IMSI Charter, la possibilità di inserire un *panic code* per azzerare l'intero contenuto del dispositivo.

Tali apparecchi sono in buona sostanza progettati per eludere le intercettazioni e per essere impiegati nel compimento di attività criminali. Tra i dispositivi maggiormente piegati a queste finalità vi sono cellulari *Iphone, Google Pixel, Blackberry* e *Nokia.*

La dotazione e la disponibilità di un criptofonino è essenziale per l'utilizzo delle **piattaforme criptate, attraverso messaggi *lockati* il cui contenuto è decifrabile esclusivamente tramite algoritmo.**

Tra le piattaforme criptate, la prima a essere stata disvelata e smantellata **è stata Encrochat**, piattaforma con server in Francia, attenzionata dalla Gendarmeria sotto la supervisione del giudice istruttore di Lille. All'esito dei primi mesi di indagine le autorità francesi accertavano che **circa il 63,7% dei criptofonini erano utilizzati per scopi criminali**. L'intercettazione dei messaggi di Encrochat si è conclusa nel giugno del 2020 quando la società si accorgeva che gli investigatori erano riusciti a bucare il sistema e quindi veniva inviato un messaggio a tutti gli utenti della piattaforma sollecitati a disfarsi dei loro cellulari.

Nel Luglio del 2020 l'indagine francese conduceva all'arresto **di 60 sospettati, al sequestro di oltre 10.000 kg di cocaina, 70 kg di eroina e 12.000 kg di cannabis, allo smantellamento di 19 laboratori di droghe, al sequestro di armi da fuoco e di 20 milioni di euro in contanti.**

Nel luglio del 2020 con un comunicato congiunto Europol e Eurojust comunicavano lo sblocco della crittografia e il monitoraggio di un'altra piattaforma denominata **SkyEcc.** Il flusso di informazioni di circa 70.000 utenti rivelava come molti utenti di Encrochat, dopo la rivelazione della avvenuta decriptazione, erano passati alla nuova piattaforma.

Le operazioni investigative che hanno portato alla luce entrambe le piattaforme si caratterizzano perché si fondano su attività di intercettazione, autorizzata secondo il diritto francese, dei server centrali.

Ebbene, attraverso **Eurojust, le Autorità francesi manifestavano la volontà di mettere a disposizione e di trasmettere tali dati ad altre A.G., ciò in quanto i dati acquisiti non riguardavano solo reti criminali operative in Francia o nei Paesi Bassi, ma anche in altri Paesi tra cui l'Italia. Le chat in questione sono state, quindi, acquisite nell'ordinamento interno tramite Ordine Europeo di indagine ai sensi della Direttiva n. 41/2024 UE e del D.lgs. n. 108/2017.**

Da qui il riferimento non può che andare, alla luce della recente esperienza del Distretto di Reggio Calabria, al procedimento convenzionalmente denominato "Eureka" che ha funto da apripista ad un intenso susseguirsi di pronunce e di orientamenti da ultimo composti dalle Sezioni Unite con le sentenze gemelle Gjuzi e Giorgi. Il procedimento Eureka avente ad oggetto delle associazioni dedite al narcotraffico, ha quale cifra identitaria l'utilizzo da parte dei sodali, per le loro comunicazioni riservate, di criptofonini di ultima generazione, in quanto ritenuti, per la loro speciale sofisticata tecnologia, non captabili da parte delle forze di polizia. Grazie all'avviata collaborazione internazionale e sulla base di formali Ordini Europei di Indagine, emessi dall'Ufficio Requirente, si è riusciti ad acquisire

ritualmente i testi delle chat criptate, intercorse nel biennio 2019-2021, sulla piattaforma SkyEcc, oggetto di sequestro da parte dell'Autorità francese.
Il procedimento Eureka così come altri affini hanno posto agli interpreti una serie di quesiti non solo meramente classificatori, ma anche concretamente operativi. Il tutto ruota sulle chat acquisite e trasmesse in provenienza dai server della piattaforma Skyecc.
Ci si è quindi chiesto quale sia la natura di tali chat, quale la disciplina loro applicabile con immediati riflessi sulla utilizzabilità, quale il vaglio rimesso al giudice dello Stato in cui le chat vengono riversate, quali i margini del diritto di difesa.
La Corte di Cassazione tra il 2022 e il 2023 ha reso numerose pronunce sulla utilizzabilità dei dati estrapolati dalle piattaforme EncroChat e Sky-ecc via OIE dalla Francia, tutte derivanti da procedimenti cautelari.

PRIMO ORIENTAMENTO: richiamo all'art. 234 BIS, trattasi di "dati freddi" per cui non è richiesta l'autorizzazione del giudice interno
Le pronunce **precedenti alle sentenze gemelle n. 44154 e 44155 del 26.10.2023**, che hanno segnato un momento di discontinuità, avevano univocamente ritenuto che **la messaggistica scambiata con i sistemi Sky Ecc ed EncroChat, acquisita mediante ordine europeo di indagine da autorità giudiziaria straniera che ne aveva eseguito la decriptazione, costituisse dato informativo documentale conservato all'estero, utilizzabile ai sensi dell'art. 234-bis cod. proc. pen., e non flusso comunicativo, non trovando applicazione la disciplina delle intercettazioni di cui agli artt. 266 e 266-bis cod. proc. pen**. (ex multis, Sez. I, n. 6363 e 6364 del 13/10/2022 Cc. -dep. 15/2/2023; Sez. IV, n. 16347 del 05/04/2023, Papalia).
Secondo un primo orientamento le chat *SKY ECC* andrebbero classificate alla stregua **di "*documenti informatici*", acquisibili ai sensi dell'art. 234 bis c.p.p. Questa tesi muove dalla distinzione tra flusso comunicativo in atto e i c.d. "*dati freddi*", ossia comunicazioni già effettuate, non più in corso ed acquisite dall'A.G. estera.** Proprio perché le chat trasmesse previo OIE dalle autorità francesi non attengono a dati in corso e in **essere, non può trovare applicazione la disciplina prevista dagli art. 266 e ss. in tema di intercettazioni, con conseguente applicazione dello statuto dell'art. 234 bis c.**p.p., che consente sempre 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*»**.**
A fronte della dizione letterale dell'art. 234bis c.p.p. si è ritenuto che "*il legittimo titolare*" sia da individuarsi nell'A.G. estera ,che quei dati detiene in forza di un autonomo e valido titolo legittimante.
Pertanto, poiché oggetto dell'OIE non sarebbe la captazione di flussi, ma di documenti l'attività sarebbe perfettamente compatibile non solo con i dettami della Direttiva 2014/41, ma anche con il D. Lgs. 108/2017, **senza alcuna necessità di "*accertare se l'autorità giudiziaria straniera abbia acquisito i dati ex post o in tempo reale, perché l'aspetto***

dirimente è costituito dall'essere stata la richiesta italiana di o.e.i. avanzata quando i flussi di comunicazione non erano più in corso".

Inoltre, non sarebbe necessaria una preventiva autorizzazione del giudice interno, neppure ai sensi dell'art. 132 del D. Lgs. 196/2003**, considerato che i dati sono stati acquisiti *ab origine* dietro provvedimento motivato dell'A.G. estera procedente**.

In tali pronunce (per tutte, Sez. IV, n. 18514, cc. 04.04.2023, dep. 4.5.2023, Puzella), **è stata superata l'eccezione di inutilizzabilità del materiale acquisito** tramite l'autorità giudiziaria francese per dedotta lesione del diritto di difesa per non essere stati messi a disposizione i provvedimenti della autorità giudiziaria francese né ivi spiegate le modalità di raccolta, rilevando che:

a) si trattava **di dati autonomamente acquisiti dalla autorità giudiziaria francese nell'ambito di procedimenti penali ivi aperti**;

b) e di **informazioni che la legislazione di quello Stato consente di tenere segrete,** la autorità giudiziaria francese non ha trasmesso la documentazione relativa alle modalità di acquisizione dei dati;

c) i diritti della difesa devono necessariamente modularsi sulla legge dello Stato che ha eseguito l'OIE, per cui, poiché, nel caso di specie, **quello Stato può legittimamente opporre il segreto sul punto, la legittimità delle modalità di acquisizione e decrittazione dei dati deve ritenersi garantita dal controllo che su quella attività è stato compiuto dall'autorità giudiziaria francese**;

d) **si è comunque attestata – con processo verbale redatto e sottoscritto dall'ufficiale di polizia giudiziaria francese incaricato dell'adempimento – la regolarità del trasferimento di quei dati su supporto informatico non modificabile e l'acquisizione è avvenuta con regolari O.I.E. messi a disposizione delle parti [**…].

SECONDO ORIENTAMENTO: inquadramento nell'art. 254 bis c.p.p., non si tratta di documenti preesistenti, ma di documenti acquisiti in forza delle indagini. Il richiamo ai presupposti di cui all'art. 270 c.p.p. non è sufficiente, occorre un vaglio da parte del giudice interno. Comparazione con la disciplina dei tabulati.

Altro orientamento sostenuto dalle sentenze della Sez. VI, n. 44154/23 e 44155/23 del 26/10/2023 ha **invece escluso l'operatività dell'art. 234-bis c.p.p., ritenendola giustificata solo per l'acquisizione di documenti e dati informatici "dematerializzati", cioè preesistenti all'avvio delle indagini da parte dell'autorità giudiziaria francese** ovvero che erano stati formati al di fuori di quelle investigazioni. Nei casi in esame, di contro, **gli elementi erano stati raccolti attraverso le indagini della autorità straniera e in forma di apprensione occulta del contenuto archiviato in un server. Tale attività acquisitiva, pertanto, andrebbe inquadrata nelle disposizioni su perquisizioni e sequestri, in specie nell'alveo dell'art. 254-bis c.p.p., riguardante il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di comunicazioni**.

Quindi, in linea con gli interventi sulla acquisizione dei dati "esterni" al traffico telefonico o telematico (nuovo art. 132 d.lgs. 196/2003, alla luce della sentenza CGUE 2.3.2021 C - 746/18), le due pronunce hanno concluso che:

a) l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione, quali quelle in esame**, debba essere sempre autorizzata da un giudice**;

b) sebbene attraverso gli OIE in esame si acquisisca **una prova precostituita – nella specie esiti di intercettazioni – il mero richiamo all'articolo 270 c.p.p. (utilizzabilità delle intercettazioni in un diverso procedimento sempre che siano indispensabili ai fini dell'accertamento dei reati indicati nell'art. 266 comma 2 bis c.p.p.) non esaurisce la verifica della sussistenza delle condizioni di ammissibilità della prova che la direttiva OIE riserva allo Stato di emissione. La natura del mezzo di prova (intercettazioni) attivato nel Paese richiesto impone, pertanto, che il giudice italiano (il GIP e, in mancanza, il riesame) verifichi, ai fini della utilizzabilità dei materiali informativi acquisiti, se sussistevano le condizioni per la autorizzabilità in sede giurisdizionale delle relative attività investigative oggetto dell'OIE**.

In particolare, secondo tale più rigida impostazione, **considerato che anche nell'ipotesi di acquisizione dei dati "*esterni*" del traffico telefonico o telematico verrebbe in rilievo quanto previsto dall'art. 132 D. Lgs. 196/2003 (che, oggi, prevede l'autorizzazione del Giudice), allora anche «*l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione deve essere sempre autorizzata da un giudice: sarebbe davvero singolare ritenere che per l'acquisizione dei dati esterni del traffico telefonico e telematico sia necessario un preventivo provvedimento autorizzativo del giudice, mentre per compiere il sequestro di dati informatici riguardanti il contenuto delle comunicazioni oggetto di quel traffico sia sufficiente un provvedimento del pubblico ministero*».**

Quindi, secondo tale tesi, se è vero che il Pubblico Ministero è sicuramente competente a richiedere tali dati tramite OIE, è altrettanto vero che tale richiesta dovrebbe essere in ogni caso preceduta da una preventiva autorizzazione del Giudice.

TERZO ORIENTAMENTO: corrispondenza telematica sequestrabile dal p.m.

Una successiva sentenza (cfr. Sez. VI, n. 46482 del 27/9/2023, dep. 17/11/2023, e simile la n. 46833 del 26/10/2023, dep. 21/11/2023) ha adottato un indirizzo ulteriormente diverso, recependo, dalle due ultime decisioni sopra richiamate, **la qualificazione dei dati raccolti all'estero come corrispondenza telematica, ma traendone conclusioni diverse in ordine alla necessità o meno di autorizzazione preventiva del giudice e su altri profili.**

La Corte muove dalla sentenza della **Corte costituzionale n. 170/2023, secondo cui anche la messaggistica – informatica o cartacea – conservata dopo la consegna non ha natura di generico documento, bensì mantiene il suo carattere di "*corrispondenza*"** così permanendo l'interesse alla riservatezza «almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, trasformandosi in un mero documento storico». Osserva, dunque, la Corte che la messaggistica sulle chat criptate in esame,

costituendo del pari registrazione di conversazioni già avvenute e, quindi, di dati "statici", è assimilabile alla corrispondenza, **la quale [giova qui aggiungere, allo stato della legislazione] non necessita di un provvedimento del giudice, potendo essere acquisita con decreto motivato di sequestro probatorio disposto dal pubblico ministero.**

La Corte puntualizza che non può, invece, invocarsi l'art. 234-bis c.p.p. sui "documenti informatici"; vero è che tanto la corrispondenza quanto i documenti informatici rientrano nel fuoco dei documenti (art. 234 c.p.p.), ma l'art. 234-bis c.p.p. ai sensi del quale *«è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico»,* fa riferimento a una specifica e diversa gamma di documenti, appunto, che intende rendere acquisibili al di fuori di qualsiasi formalità: ovvero, qualsiasi materiale disponibile in rete, con il limite che, quando si tratti di documentazione non liberamente accessibile al pubblico (per accesso protetto), il "*legittimo titolare*" autorizzi l'uso.

Conclude la Corte che **l'OIE con cui venga richiesto il trasferimento di intercettazioni di conversazioni già disposte dal giudice straniero può, dunque, essere emesso dal pubblico ministero, poiché gli atti di indagine richiesti nell'O.E.I. avrebbero potuto essere emessi alle stesse condizioni "in un caso interno analogo", segnatamente nella forma del sequestro probatorio di documentazione/corrispondenza con provvedimento del pubblico ministero.**

QUARTO ORIENTAMENTO: il *discrimen* tra dati freddi e flussi in corso. Se trattasi di messaggi conservati in server si versa nell'ipotesi di corrispondenza acquisibile ex art. 234 c.p.p., se trattasi di vera e propria attività intercettiva si applica il regime ex art. 270 c.p.p.

Infine, una terza tesi escludeva che l'acquisizione delle chat *SKY ECC* dovesse passare da un preventivo controllo del Giudice, **tanto nel caso in cui la stessa avesse ad oggetto messaggi conservati in determinati archivi e/o server, quanto nell'ipotesi di risultanze di una vera e propria attività intercettativa.**

Difatti, nel primo caso, **i dati avrebbero natura documentale sub specie "*corrispondenza*", certamente acquisibili ai sensi dell'art. 234 c.p.p.; nel secondo caso, invece, la norma di riferimento sarebbe l'art. 270 c.p.p., il quale parimenti consente la circolarità delle intercettazioni in diversi procedimenti.**

Inoltre, pure tale ultima teoria concludeva per la piena compatibilità dell'attività di acquisizione mediante OIE con le norme nazionali e comunitarie, non soltanto in ragione dei principi di presunzione di legittimità delle operazioni eseguite dall'A.G. di esecuzione e di reciproco affidamento tra Stati membri, ma anche per il raggiungimento della prova positiva della piena legittimità di tutte le operazioni, atteso che:

*a) **la disciplina francese in materia di acquisizione della messaggistica già trasmessa e conservata nei dispositivi personali mediante accesso occulto a sistemi informatici (artt. da 706-95 a 706-95-3 e da 706-102-1 a 706-102-5 del codice di procedura penale) prevede la necessità di un provvedimento motivato del giudice;***

b) la segretezza del sistema usato per "mettere in chiaro" i messaggi criptati ***non è in contrasto con la legge italiana, perché gli artt. 268 cod. proc. pen. e 89 disp. att. cod. proc. pen. riconoscono il diritto di accedere al verbale delle operazioni e alle registrazioni, ma non anche ai mezzi tecnici e ai programmi utilizzati per la intrusione nelle conversazioni intercettate;***

c) la decriptazione delle conversazioni e comunicazioni è attività distinta dalla captazione, e, quindi, non implica il diritto di conoscere il programma o l'algoritmo a ciò necessario, salvo che siano allegate e provate specifiche anomalie tecniche".

L'INTERVENTO DELLE SEZIONI UNITE, sentenze n. 23755 e 23756 del 29.2.2024:

Alla luce di tale contrasto interpretativo sorto e riassunto nei termini che precede, la questione è stata rimessa al vaglio delle Sezioni Unite.

Per la precisione, i quesiti sottoposti e risolti dalla **sentenza a Sezioni Unite Gjuzi** n. 23755/2024 del 29.2.2024 sono i seguenti:

- ***a)*** *se l'acquisizione di messaggi su chat di gruppo scambiati con sistema cifrato attraverso un ordine europeo di indagine rivolto ad un'autorità giudiziaria straniera che ne abbia eseguito la decrittazione costituisca* ***acquisizione di documenti e di dati informatici ai sensi dell'art. 234-bis cod. proc. pen. o di documenti ex art. 234 cod. proc. pen. ovvero sia riconducibile ad altra disciplina relativa all'acquisizione di prove;***
- ***b)*** ***se l'acquisizione di cui sopra debba essere oggetto, ai fini della utilizzabilità dei relativi dati, di preventiva o successiva verifica giurisdizionale della sua legittimità da parte della autorità giurisdizionale nazionale.***

Queste, invece, le soluzioni adottate dalla sentenza:

- "*La trasmissione, richiesta con ordine europeo di indagine, del contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa,* ***non rientra nell'ambito di applicazione dell'art. 234-bis cod. proc. pen., che opera al di fuori delle ipotesi di collaborazione tra autorità giudiziarie, bensì nella disciplina relativa alla circolazione delle prove tra procedimenti penali, quale desumibile dagli artt. 238 e 270 cod. proc. pen. e 78 disp. att. cod. proc. pen.***". **E, invero, l'art. 234 bis c.p.p. "*** ***disciplina non un mezzo di prova, bensì una modalità di acquisizione di particolari*** ***tipologie di elementi di prova presenti all'estero, che viene attuata in via "diretta" dall'autorità giudiziaria italiana e prescinde da qualunque forma di collaborazione con le autorità dello Stato in cui tali dati sono custoditi"; invece la disciplina in tema di OIE – pur avendo ad oggetto una prova formatasi all'estero – prevede necessariamente una forma di collaborazione tra Stati, nel senso che il dato probatorio entra nel nostro ordinamento soltanto in forza di una necessaria interlocuzione con l'A.G. dello Stato estero presso cui la prova si trova**.

- "***In materia di ordine europeo di indagine, le prove già in possesso delle autorità competenti dello Stato di esecuzione possono essere legittimamente richieste ed acquisite dal pubblico ministero italiano senza la necessità di preventiva***

autorizzazione da parte del giudice del procedimento nel quale si intende utilizzarle".

- "*L'emissione, da parte del pubblico ministero,* ***di ordine europeo di indagine diretto ad ottenere il contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, non deve essere preceduta da autorizzazione del giudice italiano, quale condizione necessaria a norma dell'art. 6 Direttiva 2014/41/UE, perché tale autorizzazione, nella disciplina nazionale relativa alla circolazione delle prove, non è richiesta per conseguire la disponibilità del contenuto di comunicazioni già acquisite in altro procedimento".***
- "***La disciplina di cui all'art. 132 d.lgs. n. 196 del 2003, relativa all'acquisizione dei dati concernenti il traffico di comunicazioni elettroniche e l'ubicazione dei dispositivi utilizzati, si applica alle richieste rivolte ai fornitori del servizio, ma non anche a quelle dirette ad altra autorità giudiziaria che già detenga tali dati, sicché, in questo caso, il pubblico ministero può legittimamente accedere agli stessi senza chiedere preventiva autorizzazione al giudice davanti al quale intende utilizzarli***".
- "***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 trasmesse 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, fermo restando che l'onere di allegare e provare i fatti da cui inferire tale violazione grava sulla parte interessata***".
- "***L'impossibilità per la difesa di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per criptare il testo delle stesse non determina una violazione dei diritti fondamentali, dovendo escludersi, salvo specifiche allegazioni di segno contrario, il pericolo di alterazione dei dati in quanto il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, ed una chiave errata non ha alcuna possibilità di decriptarlo anche solo parzialmente".***

Le questioni decise dalle Sezioni Unite con la **sentenza Giorgi** n. 23756/2024 del 29.2.2024 erano, invece, le seguenti:

- "*Se l'acquisizione di messaggi su chat di gruppo, scambiati con sistema cifrato, attraverso un ordine europeo di indagine presso un'autorità giudiziaria straniera che ne abbia eseguito la decrittazione costituisca acquisizione di* ***documenti e di dati informatici ai sensi dell'art. 234-bis cod. proc. pen. o di documenti ex art. 234 cod. proc. pen. ovvero sia riconducibile ad altra disciplina relativa all'acquisizione di prove***";
- "*Se l'acquisizione di cui sopra debba essere oggetto, ai fini della utilizzabilità dei relativi dati, di* ***preventiva o successiva verifica giurisdizionale della sua legittimità da parte della autorità giurisdizionale nazionale***".
- ***"Se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera su una piattaforma informatica criptata integri l'ipotesi disciplinata nell'ordinamento interno dall'art. 270 cod. proc. pen.***";

- "*Se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera attraverso l'inserimento di un* ***captatore informatico sui server di una piattaforma criptata sia soggetta nell'ordinamento interno a un controllo giurisdizionale, preventivo o successivo, in ordine all'utilizzabilità dei dati raccolti***".

Di seguito le soluzioni adottate:

- "*In materia di ordine europeo di indagine, 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 e su criptofonini,* ***non rientra nell'ambito di applicazione dell'art. 234-bis cod. proc. pen., che opera al di fuori delle ipotesi di collaborazione tra autorità giudiziarie, ma è assoggettata alla disciplina di cui all'art. 270 cod. proc. pen.".***
- "*In materia di ordine europeo di indagine,* ***le prove già in possesso delle autorità competenti dello Stato di esecuzione possono essere legittimamente richieste ed acquisite dal pubblico ministero italiano*** *senza la necessità di preventiva autorizzazione da parte del giudice del procedimento nel quale si intende utilizzarle*".
- "*L'emissione, da parte del pubblico ministero, di ordine europeo di indagine diretto ad ottenere i risultati di intercettazioni disposte da un 'autorità giudiziaria straniera in un procedimento penale pendente davanti ad essa, ed effettuate attraverso l'inserimento di un* ***captatore informatico sui server di una piattaforma criptata, è ammissibile, perché attiene ad esiti investigativi ottenuti con modalità compatibili con l'ordinamento italiano, e non deve essere preceduta da autorizzazione del giudice italiano, quale condizione necessaria ex art. 6 Direttiva 2014/41/UE, perché tale autorizzazione non è richiesta nella disciplina nazionale***".
- "***L'utilizzabilità 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 e su criptofonini, deve essere esclusa se il giudice del procedimento nel quale dette risultanze istruttorie vengono acquisite rileva che, in relazione ad esse, si sia verificata la violazione dei diritti fondamentali, fermo restando che l'onere di allegare e provare i fatti da cui in ferire tale violazione grava sulla parte interessata".***
- "***L 'impossibilità per la difesa di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per criptare il testo delle stesse non determina una violazione dei diritti fondamentali, dovendo escludersi, salvo specifiche allegazioni di segno contrario, il pericolo di alterazione dei dati in quanto il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, ed una chiave errata non ha alcuna possibilità di decriptarlo anche solo parzialmente".***

***

Ebbene, le decisioni sopra riportate sono state adottate dalle Sezioni Unite dopo un'attenta disamina degli orientamenti giurisprudenziali sopra esposti e un confronto con la normativa di riferimento, vale a dire la Direttiva UE 2014/41 e il D. Lgs. 108/2017 in materia di Ordine Europeo di Indagine.

Le Sezioni Unite prendono le mosse dal dato certo che tanto la Direttiva 2014/41 quanto il D. Lgs. 108/2017 sono entrambi naturalmente improntati al rispetto dei diritti fondamentali nazionali e comunitari, tra cui – ovviamente – anche il diritto di difesa e quello del giusto processo.

Tuttavia, ai fini del rispetto di simili canoni non è necessario che lo Stato di esecuzione, presso cui è richiesta la prova, abbia acquisito quest'ultima nell'osservanza anche della disciplina nazionale di riferimento in tema di formazione ed acquisizione delle prove.

Anzi, secondo la Corte, **l'art. 14 della Direttiva garantisce allo Stato estero di esecuzione la propria primazia nell'applicazione delle sue regole procedurali**.

Per queste ragioni, la Corte ha escluso che la mancata e pedissequa osservanza all'estero dei medesimi canoni previsti dalla legislazione nazionale in tema di prove possa comportare l'inutilizzabilità degli atti acquisiti mediante OIE: "*questa Corte ha altresì affermato che, in materia di rogatoria internazionale,* ***l'atto istruttorio assunto all'estero è inutilizzabile solo quando venga prospettata l'assenza nell'ordinamento dello Stato richiesto di una normativa a tutela delle garanzie difensive, non anche quando si contesti la mera inosservanza delle regole dettate dal codice di rito dello Stato italiano richiedente (Sez. 6, n. 43534 del 24/04/2012, Lubiana, Rv. 253797 - 01)".***

Sempre con riferimento al rispetto dei principi fondamentali, le Sezioni Unite hanno dato atto di come, in ambito di cooperazione giudiziaria europea, sussista la presunzione di legittimità dell'operato dello Stato estero in forza del principio di reciproco affidamento tra Stati membri.

Trattasi, invero, di enunciazioni espressamente previste dalla Direttiva, considerato che ogni Stato europeo è tenuto al rigoroso rispetto dei diritti elencati nella Carta di Nizza; ciononostante trattasi di presunzione relativa, la cui prova contraria spetta alla Parte che intende denunciare una simile violazione: "***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 o.e.i***.".

***

Entrando nel vivo dell'argomento, la Corte di Cassazione affronta poi il problema della messaggistica *SKY ECC* acquisita tramite OIE e della sua compatibilità con i principi ora esposti.

Nel far ciò, i giudici di legittimità hanno dovuto dirimere la questione preliminare relativa alla natura giuridica dei messaggi scambiati su tale rete di comunicazione, poiché soltanto dopo aver individuato il "*tipo*" di atto richiesto è possibile **verificare non solo il rispetto dei diritti fondamentali, ma anche il rispetto del c.d. criterio di reciprocità stabilito dall'art. 6 Dir. 2014/41, che ammette l'OIE soltanto nel caso in cui l'atto richiesto sia ammissibile anche in un "*caso analogo*" nel diritto interno**.

Orbene, in primo luogo la Suprema Corte ha escluso che **l'acquisizione di messaggi scambiati su chat criptate possa ricondursi nell'alveo della disciplina applicabile ai**

documenti informatici di cui all'art. 234 bis c.p.p., trattandosi di normativa alternativa e incompatibile con quella in tema di OIE.

E, invero, l'art. 234 bis c.p.p. "*disciplina non un mezzo di prova, bensì una modalità di acquisizione di particolari* tipologie di elementi di prova presenti all'estero, che viene attuata in via "*diretta" dall'autorità giudiziaria italiana e prescinde da qualunque forma di collaborazione con le autorità dello Stato in cui tali dati sono custoditi*"; diversamente, la disciplina in tema di OIE – pur avendo ad oggetto una prova formatasi all'estero – postula necessariamente una forma di collaborazione tra Stati, nel senso che il dato probatorio entra nel nostro ordinamento soltanto in forza di una necessaria interlocuzione con l'A.G. dello Stato estero presso cui la prova si trova.

Tanto chiarito, le Sezioni Unite hanno preso le mosse da un dato del tutto incontrastato e cioè che i messaggi intercorsi sulle **chat *SKY ECC* costituiscono già "*prove*" ottenute ed acquisite in altro procedimento penale estero.**

Quindi, trattandosi di prove già a disposizione dell'A.G. estera **verrebbero in rilievo tanto gli artt. 10 e 12 della Direttiva (che prevedono un meccanismo più agevole per accelerare lo scambio informativo), quanto le norme nazionali in tema di "*circolazione*" delle prove in altri procedimenti, vale a dire gli artt. 238 e 270 c.p.p., nonché l'art. 78 disp. att. c.p.p.**

Queste ultime, in particolare, **disciplinando la sola circolazione delle prove prevedono una disciplina diversa e, per certi versi, più snella rispetto a quelle disciplinanti la "*formazione*" delle prove stesse.**

Difatti, in via generale, può dirsi che nel nostro ordinamento è certamente consentito al Pubblico Ministero o alla Parte che vi ha interesse produrre prove formatesi in altri giudizi, senza alcuna preventiva autorizzazione da parte del Giudice procedente.

Quest'ultimo, infatti, è soltanto chiamato a valutare l'ammissibilità degli atti e la loro utilizzabilità ai fini della decisione.

In particolare, si legge in sentenza: "*questo assetto normativo si ricava con chiarezza dal sistema costituito dagli artt. 238 e 270 cod. proc. pen. e 78 disp. att. cod. proc. pen.*

***L'art. 238 cod. proc. pen. detta le regole generali in tema di circolazione dei verbali di prove di altri procedimenti**. La disciplina in esso contenuta, che si riferisce espressamente anche agli atti non ripetibili, non prevede, ai fini dell'acquisizione delle prove formate altrove, alcun intervento preventivo da parte del giudice del procedimento nel quale si vorrebbero utilizzarle. **La norma si preoccupa unicamente di fissare condizioni per l'utilizzazione di prove provenienti da altri procedimenti; e, tra queste condizioni, si ribadisce, non è ricompresa la previa autorizzazione**.*

***L'art. 270 cod. proc. pen., a sua volta, indica i requisiti per l'utilizzazione dei risultati delle intercettazioni di conversazioni o di comunicazioni in procedimenti diversi da quelli nei quali le stesse sono state disposte**. Anche questa disciplina, speciale rispetto a quella di cui all'art. 238 cod. proc. pen. perché riferita ad uno specifico mezzo di ricerca della prova, **non prevede alcun intervento autorizzativo preventivo del giudice del procedimento di "destinazione", che abbia la funzione di autorizzare le parti interessate a procedere all'acquisizione di copia dei relativi atti**. L'art. 270, comma 2, cod. proc. pen., infatti, stabilisce che, ai fini della utilizzazione dei risultati di intercettazioni effettuate in procedimenti diversi, le parti interessate hanno l'onere di*

depositare i verbali e le registrazioni a queste relativi, senza però contenere alcun riferimento ad autorizzazioni preventive del giudice del processo di "destinazione" per ottenere la disponibilità di tali atti. ***Inoltre, forse ancor più significativamente, l'art. 270, comma 3, cod. proc. pen., riconosce al pubblico ministero e ai difensori delle parti interessate «la facoltà di esaminare i verbali e le registrazioni in precedenza depositati nel procedimento in cui le intercettazioni furono autorizzate», sempre senza prevedere autorizzazioni preventive del giudice del processo di "destinazione"****.*

L'art. 78 disp. att. cod. proc. pen*., rubricato «Acquisizione di atti di un procedimento penale straniero», ancora, dispone, in linea generale, al comma 1, che «[l]a documentazione di atti di un procedimento penale compiuti da autorità giudiziaria straniera* ***può essere acquisita a norma dell'art. 238 del codice****», e si limita ad aggiungere, al comma 2, che, per gli atti non ripetibili compiuti dalla polizia straniera, l'acquisizione nel fascicolo per il dibattimento è subordinata al previo esame in contraddittorio dell'autore degli stessi, o al consenso delle parti*".

Quindi, sulla scorta della disciplina comunitaria e di quella interna, **le Sezioni Unite hanno escluso che l'acquisizione di prove di altri procedimenti debba necessariamente passare per una preventiva autorizzazione da parte del Giudice che procede, ciò non essendo richiesto da alcuna disposizione.**

Inoltre, sul versante europeo, pure **la Corte EDU ha escluso che l'art. 8 CEDU esiga l'autorizzazione *ex ante* di un giudice per la circolazione delle intercettazioni da un procedimento all'altro**.

Pertanto, **l'unico criterio di ammissibilità previsto ai sensi dell'art. 6 della Direttiva è che la prova possa essere legittimamente richiesta "*in un caso analogo*".**

Tale criterio, allora, secondo le Sezioni Unite risulta pienamente soddisfatto poiché - come si è visto - è certamente consentito al Pubblico Ministero e alle altre Parti interessate presentare prove provenienti da altri procedimenti.

Una volta, però, che le prove sono legittimamente presentate nel procedimento interno spetta sempre al Giudice il potere di valutare la loro ammissibilità e utilizzabilità ai fini della decisione.

E sarebbe proprio in questa fase, prosegue la Corte, che la Parte che denuncia eventuali vizi degli atti acquisiti tramite OIE dovrebbe espressamente impugnare tale atto, fornendo adeguata allegazione dei fatti da cui desumere una violazione dei diritti fondamentali.

Proseguendo ed entrando nel merito dei ricorsi sottoposti all'attenzione delle Sezioni Unite, esse affrontano specificamente i rilievi difensivi secondo cui i messaggi scambiati sulla piattaforma *SKY ECC* sarebbero inquadrabili come risultanze di un'attività di intercettazione.

Nel vagliare le argomentazioni della difesa, **la Corte ravvisa nell'art. 270 c.p.p. il parametro normativo di riferimento.**

Ora, la **norma citata ammette la circolazione dell'attività captativa a condizione che essa "*risulti rilevante ed indispensabile per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza*".**

Sulla scorta del dato normativo, le Sezioni Unite evidenziano in primo luogo che per la circolazione delle intercettazioni è sufficiente e necessaria una richiesta del Pubblico Ministero (o della Parte interessata) senza alcuna autorizzazione del Giudice.
In secondo luogo, precisano anche che non è causa di nullità e/o inutilizzabilità l'omesso deposito degli atti del procedimento originario: "*numerose decisioni, poi, affermano che, **in tema di intercettazioni disposte in altro procedimento, l'omesso deposito degli atti relativi, ivi compresi i nastri di registrazione, presso l'autorità competente per il diverso procedimento, non ne determina l'inutilizzabilità, in quanto detta sanzione non è prevista dall'art. 270 cod. proc. pen. e non rientra nel novero di quelle di cui all'art. 271 cod. proc. pen. aventi carattere tassativo** (così ex plurimis: Sez. 5, n. 1801 del 16/07/2015, dep. 2016, Tunno, Rv. 266410 - 01; Sez. 5, n. 14783 del 13/03/2009, Badescu, Rv. 243609 - 01; Sez. 6, n. 27042 del 18/02/2008, Morabito, Rv. 240972 - 01)*".
Infine, concludono affermando che spetta sempre alla Parte interessata produrre gli atti cui le intercettazioni si riferiscono al fine di eccepire eventuali vizi.
Sul versante comunitario, invece, la disciplina di riferimento è stata individuata in quella prevista dagli artt. 30 e 31 della Direttiva 2014/41 che disciplinano proprio il caso delle intercettazioni eseguite mediante OIE.
Nello specifico, l'art. 30 stabilisce che «*l'autorità di emissione può altresì richiedere, se ne ha particolare motivo, una trascrizione, una decodificazione o una decrittazione della registrazione, fatto salvo l'accordo dell'autorità di esecuzione*».
L'art. 31, invece, prevede una particolare forma di collaborazione tra Stati, tenuto conto che lo Stato in cui le operazioni di intercettazione sono eseguite, nel momento in cui viene a conoscenza che "*l'indirizzo di comunicazione della persona soggetta a intercettazione indicata nell'ordine di intercettazione è utilizzato sul territorio di un altro Stato membro*" dovrà procedere a darne pronta comunicazione a quest'ultimo.
Lo Stato interessato, allora, "***può comunicare che l'intercettazione non è consentita**; in questi casi, l'attività non può essere iniziata o proseguire, e gli eventuali risultati già ottenuti mentre la persona soggetta ad intercettazione si trovava sul territorio dello Stato che ha ricevuto la «notifica» non possono essere utilizzati, o possono esserlo solo alle condizioni specificate dall'autorità competente di quest'ultimo*".
Ancora, il D. lgs. 108/2017 attuativo della Direttiva medesima disciplina le operazioni di intercettazione agli artt. 43 e 44 per le procedure attive e agli artt. 23 e 24 per quelle passive. Le prime due norme sono sostanzialmente sovrapponibili a quelle comunitarie.
Al contrario, l'art. 24 prevede quale unico divieto sanzionato con l'inutilizzabilità il caso in cui "***le intercettazioni sono state disposte in riferimento a un reato per il quale, secondo l'ordinamento interno, le stesse non sono consentite***".
Pertanto, le Sezioni Unite hanno ritenuto la compatibilità delle chat acquisite mediante OIE e costituenti già prova in altro procedimento **con il principio sancito dall'art. 6 Dir. 2014/41, tenuto conto che** "***il divieto della Direttiva 2014/41/UE di iniziare o proseguire le attività di captazione, ovvero di utilizzarne i risultati, è previsto solo «[q]ualora l'intercettazione non sia ammessa in un caso interno analogo». E, nella disciplina italiana di attuazione***

della Direttiva cit., l'art. 24 d.lgs. n. 108 del 2017 prevede un'unica ipotesi vietata: «se le intercettazioni sono state disposte in riferimento a un reato per il quale, secondo l'ordinamento interno, le intercettazioni non sono consentite».

Può quindi concludersi che, nell'ordinamento italiano, sulla base della disciplina di cui all'art. 31 Direttiva 2014/41/UE, ***l'inutilizzabilità dei risultati di intercettazioni disposte da autorità di altro Stato ed effettuate nei confronti di persone il cui «indirizzo di comunicazione» è attivato in Italia sussiste solo se l'autorità giudiziaria italiana rileva che le captazioni non sarebbero state consentite «in un caso interno analogo», perché disposte per un reato per il quale la legge nazionale non prevede la possibilità di ricorrere a tale mezzo di ricerca della prova***".

Ebbene, nel caso sottoposto all'attenzione delle Sezioni Unite le intercettazioni erano certamente consentite in un "*caso analogo interno*".

Difatti, innanzi all'A.G. francese si procedeva per reati in tema di stupefacenti e, per la precisione, erano stati attenzionati soggetti facenti parte di vaste organizzazioni criminali dedite al narcotraffico.

Inoltre, **la violazione del sistema di comunicazione *SKY ECC* costituiva metodo di indagine indispensabile per l'accertamento dei fatti, atteso che i vari indagati utilizzavano proprio le chat criptate per la perpetrazione degli illeciti.**

Procedendo oltre, le Sezioni unite hanno affrontato, anche l'ulteriore questione della compatibilità con il diritto interno delle intercettazioni disposte dall'A.G. francese sui server di *SKY ECC* eseguite mediante l'installazione di un captatore informatico al fine di acquisire le chiavi di cifratura delle comunicazioni, custodite nei dispositivi dei singoli utenti.

Al riguardo, si legge in sentenza: "***in proposito, non assume valenza dirimente il fatto che, nel codice di rito, in materia di intercettazioni, si faccia menzione della sola ipotesi dell'«inserimento di un captatore informatico su un dispositivo elettronico portatile»***.

Il captatore informatico, infatti, non è un autonomo mezzo di ricerca della prova, e tanto meno un mezzo di prova, bensì uno strumento tecnico attraverso il quale esperire il mezzo di ricerca della prova costituito dalle intercettazioni di conversazioni o di comunicazioni.

Sicché non è indispensabile che il legislatore preveda dove lo stesso possa essere "inserito".

E una conferma di questa conclusione può essere desunta dall'elaborazione della giurisprudenza di legittimità, anche delle Sezioni Unite, la quale, già prima che venisse previsto dalla legge l'utilizzo del captatore informatico come strumento per effettuare attività di intercettazione, ne aveva ritenuto legittimo l'impiego a tali fini, precisandone anche l'ammissibilità, nei procedimenti per delitti di criminalità organizzata, con riguardo a captazioni di conversazioni o comunicazioni tra presenti in luoghi di privata dimora (così, per tutte, Sez. U, n. 26889 del 28/04/2016, Scurato, Rv. 266905 - 01)".

Inoltre, non è stata ravvisata alcuna incompatibilità neppure sul versante comunitario, atteso che "***per un verso, sia la Direttiva 2014/41/UE, all'art. 30, paragrafo 7, sia il d.lgs. n. 108 del 2017, all'art. 43, comma 4, prevedono espressamente la possibilità per l'autorità che ha emesso un o.e.i. per l'intercettazione di telecomunicazioni di chiedere la decodificazione o la decrittazione delle comunicazioni intercettate. E così disponendo, riconoscono che***

l'attività di intercettazione implica anche l'acquisizione degli strumenti necessari per procedere a decodificazione o decrittazione delle conversazioni o comunicazioni".
In altri termini, secondo la Cassazione il c.d. trojan non sarebbe altro che uno strumento tecnico ed attuativo necessario per la corretta esecuzione dell'attività captativa.
Resta comunque fermo il fatto che - nel disporre simili operazioni dotate di intrinseca ed indiscussa intrusività - è necessario che vi sia stata una preventiva autorizzazione del Giudice del procedimento in cui la prova è stata raccolta.
Ciò, tra l'altro, è quanto richiesto anche dalla giurisprudenza della Corte EDU, la quale richiede una disciplina il più possibile chiara sui suoi presupposti applicativi e il ricorso a mezzi tanto incisivi soltanto in presenza della commissione di gravi reati e in caso di inadeguatezza di altre tecniche di indagine.
In altri termini, si assisterebbe ad una violazione dei diritti fondamentali soltanto in caso di intercettazioni disposte fuori dai casi previsti dalla legge e in assenza di un provvedimento motivato del Giudice.
Tuttavia, ciò non si sarebbe verificato nel "*caso francese*", considerato che le intercettazioni dei messaggi di gruppo scambiati sulle chat *SKY ECC* mediante installazione di un captatore informatico sui server della società canadese sono avvenute dietro provvedimento motivato del Giudice francese e sotto il suo diretto controllo, nel pieno rispetto delle norme previste dal codice di rito francese e in conformità ai canoni comunitari in tema di giusto processo e diritto di difesa.
Quanto, poi**, all'omessa conoscenza dell'algoritmo utilizzato per decrittare le conversazioni, anche in tal caso la Cassazione ha escluso che ciò possa comportare una violazione dei principi del giusto processo e del diritto di difesa.**
Difatti, le chiavi di decrittazione – oltre a riguardare aspetti meramente esecutivi e tecnici dell'attività di captazione – non comporterebbero alcuna alterazione del dato estrapolato, considerato che in presenza di una chiave errata sarebbe del tutto impossibile decifrare (anche solo parzialmente) il contenuto della chat.
Ad ogni modo, anche in questo caso, la Corte fa comunque salva la possibilità di specifiche allegazioni di segno contrario da parte della Difesa.
In particolare, si legge in sentenza: "***Nemmeno l'impossibilità, per la difesa, di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per "criptare" il contenuto delle stesse determina, almeno in linea di principio, una violazione di «diritti fondamentali».*** *Ed infatti, se è vero che la disponibilità dell'algoritmo di criptazione è funzionale al controllo dell'affidabilità del contenuto delle comunicazioni acquisite al procedimento, deve però osservarsi, in linea con quanto evidenziato da numerose decisioni, 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*** *(cfr., tra le tante: Sez. 6, n. 46833 del 26/10/2023, Bruzzaniti, non mass. sul punto; Sez. 6 n. 48838 dell'11/10/2023, Brunello, non mass. sul punto; Sez. 4, n. 16347 del 05/04/2023, Papalia, non mass. sul punto; Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Calderon, non mass. sul punto).* ***Né la***

giurisprudenza sovranazionale risulta aver affermato che l'indisponibilità dell'algoritmo di decriptazione agli atti del processo costituisca, di per sé, violazione dei «diritti fondamentali». *In proposito, anzi, può rilevarsi che* ***la Corte EDU****, pronunciandosi in relazione ad una vicenda in cui i dati acquisiti non erano stati messi a disposizione della difesa e la pronuncia di colpevolezza era stata fondata sul mero fatto dell'uso di un sistema di messaggistica criptata denominato ByLock,* ***si è limitata ad affermare che dare al ricorrente l'opportunità di prendere conoscenza del materiale decriptato nei suoi confronti poteva costituire un passo importante per preservare i suoi diritti di difesa senza avere, al contempo, affermato che tale mancata messa a disposizione integrasse un vulnus dei diritti fondamentali*** *(Corte EDU, Grande Camera, 26/09/2023, Yiiksel YalOnkaya c. Turchia, g 336; il testo originale è il seguente: «The Court is accordingly of the view that giving the applicant the opportunity to acquaint himself with the decrypted ByLock material in his regard would have constituted an important step in preserving his defence rights»).*

In ogni caso, inoltre, resta fermo che l'onere dell'allegazione e della prova in ordine ai fatti da cui desumere la violazione dei «diritti fondamentali» grava sulla parte interessata*, per le ragioni indicate in precedenza nel par. 10.6*".

Infine, occorre dare conto di quanto statuito dalle Sezioni Unite nella sentenza Gjuzi, sullo specifico tema dei dati del traffico telefonico e telematico acquisiti mediante OIE (tabulati telefonici e geolocalizzazione).

Com'è noto, infatti, a seguito della riforma dell'art. 132 D. Lgs. 196/2003 anche per l'acquisizione di tali dati è, oggi, necessaria la preventiva autorizzazione del Giudice, in conformità a quanto richiesto dal diritto europeo.

Tuttavia, secondo le Sezioni Unite, nel momento in cui tali dati sono stati già acquisiti dall'A.G. estera (dietro provvedimento del Giudice, nel rispetto della procedura di riferimento e dei diritti fondamentali), non è prevista alcuna preventiva autorizzazione da parte dell'A.G. italiana per la loro acquisizione tramite OIE ai fini dell'utilizzabilità nel procedimento interno.

Difatti, alla luce di un'interpretazione sistematica delle disposizioni contenute nell'art. 132 D. Lgs. 196/2003 l'autorizzazione del Giudice si rende necessaria soltanto nel caso di "*acquisizione dei dati presso il gestore dei servizi telefonici e telematici, ma non anche all'utilizzazione dei dati in un procedimento penale diverso da quello in cui sono stati già acquisiti*".

Quindi, nel caso in cui **i dati del traffico telefonico e telematico siano già divenuti patrimonio probatorio di procedimento penale estero non si pone alcun problema di richiedere gli stessi al gestore delle telecomunicazioni, poiché essi sono stati già estrapolati dall'A.G. estera e messi a sua disposizione**.

Pertanto, osserva la Corte, "***nel sistema processuale italiano, il pubblico ministero può acquisire da altra autorità giudiziaria dati relativi al traffico o all'ubicazione, concernenti comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica, senza dover chiedere preventiva autorizzazione al giudice competente per il procedimento nel quale intende utilizzarli****, in forza dei principi generali indicati in precedenza nel § 9.2, e in difetto di regole o principi di segno diverso nella specifica materia*

(…)

*Invero, come si è detto in precedenza al § 12.2**, in questo caso l'accesso ai dati relativi al traffico e all'ubicazione, concernenti comunicazioni elettroniche, da parte dell'autorità statuale istituzionalmente preposta a dirigere le indagini, è già avvenuto in forza del preventivo controllo di un giudice a tutela dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone interessate*".

In ragione di quanto precede, così concludono le **Sezioni Unite Giorgi** sulla tenuta legale degli atti acquisiti tramite OIE: "*Ora, secondo i principi di diritto precedentemente enunciati, **anche a voler ritenere che detti atti siano qualificabili come risultati di intercettazioni di conversazioni o comunicazioni, la loro acquisizione può essere effettuata sulla base di o.e.i. emesso dal pubblico ministero in assenza di preventiva autorizzazione del giudice, in quanto tale autorizzazione non è richiesta nell'ordinamento italiano per l'utilizzazione degli esiti di intercettazioni in procedimenti diversi da quelli in cui sono state disposte**.*

*Inoltre, sempre sulla base dei principi di diritto precedentemente enunciati, **deve escludersi il mancato rispetto del requisito di cui all'art. 6, paragrafo 1, lett. b), Direttiva cit. anche a voler ritenere che l'o.e.i. abbia ad oggetto l'acquisizione dei risultati di intercettazioni effettuate attraverso l'inserimento di un captatore informatico sui server di una piattaforma criptata. Si è infatti evidenziato che questa modalità investigativa è compatibile con la disciplina delle intercettazioni prevista nell'ordinamento italiano**.*

Né vi sono dubbi che gli atti ottenuti mediante o.e.i. siano stati richiesti in quanto ritenuti «rilevanti ed indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza»

(…)

***In secondo luogo, deve ritenersi soddisfatta la condizione di ammissibilità posta dall'art. 6, paragrafo 1, lett. a), Direttiva 2014/41/UE, relativa alla necessità e proporzionalità delle attività richieste mediante o.e.i., anche in considerazione dei diritti degli indagati**.*

*Si è detto in precedenza, al § 10.2, che l'esame di tale profilo deve essere compiuto avendo riguardo al procedimento nel cui ambito è emesso l'ordine europeo di indagine. **E, nella specie, l'o.e.i. risulta formulato con espresso riferimento all'acquisizione delle comunicazioni relative a persone nominativamente indicate, tra le quali i due attuali ricorrenti, in quel momento già tutte sottoposte ad indagini per i reati di partecipazione ad associazione per delinquere finalizzata al traffico internazionale di cocaina e di acquisto, detenzione, importazione e cessione di partite di tale sostanza stupefacente**.*

(…)

***Né può dirsi che, nel presente procedimento, sia stata accertata la violazione di «diritti fondamentali»**.*

*18.5.1. **Innanzitutto, i dati probatori trasmessi dall'autorità giudiziaria francese sono stati acquisiti in un procedimento penale pendente davanti ad essa sulla base di provvedimenti autorizzativi adottati da un giudice in relazione ad indagini per gravi reati, ed ampiamente motivati in ordine all'esistenza in concreto dei presupposti ritenuti necessari dalla giurisprudenza della Corte EDU**.*

Invero, dall'esame alle ordinanze emesse dal Giudice Istruttore del Tribunale di Parigi, allegate dalla difesa alla richiesta di riesame, e prodotte in questa sede, si evince che i reati

per i quali le operazioni sono state disposte sono quelli di associazione per delinquere finalizzata al traffico di sostanze stupefacenti*, di traffico di sostanze stupefacenti, di fornitura di prestazioni di crittografia non autorizzate, e di fornitura e importazione di mezzi di crittografia non autorizzati.*

Il ricorso al sistema Sky-Ecc, inoltre, per le modalità di accesso, per la impenetrabilità dall'esterno, e per l'utilizzo che risulta esserne stato fatto, costituisce una concreta e specifica fonte indiziante a carico dei singoli utenti proprio con riguardo a tali reati.

(…)

Le medesime ordinanze, poi, anche facendo richiamo ad episodi specifici, rappresentano che il sistema Sky-Ecc è stato utilizzato da organizzazioni criminali operanti in Francia, in Belgio, nei Paesi Bassi e a livello internazionale, proprio in materia di traffico di sostanze stupefacenti. Espongono, ancora, che l'inserimento del captatore informatico sui server della piattaforma della società Sky-Ecc è da ritenere indispensabile perché 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 gestisce e conoscere i legami di costoro con le organizzazioni criminali*.*

18.5.2. Le motivazioni esposte nelle ordinanze emesse dal Giudice Istruttore del Tribunale di Parigi escludono anche la plausibilità della prospettazione secondo cui le autorità francesi avrebbero effettuato intercettazioni generalizzate ed indiscriminate.

(…)

Deve poi escludersi che l'indisponibilità delle chiavi di cifratura necessarie per rendere le comunicazioni acquisite intelligibili costituisca una violazione dei diritti di difesa e della garanzia di un giusto processo*.*

(…)

Ancora, non risulta configurabile la violazione delle garanzie previste dalla Direttiva 2014/41/UE*. Invero, anche a voler ritenere che gli atti ricevuti dall'autorità giudiziaria francese siano qualificabili come risultati di intercettazioni di conversazioni o comunicazioni,* ***deve escludersi, in forza di quanto osservato in precedenza al § 15.5.2, che sia configurabile l'unica fattispecie di inutilizzabilità prevista dalla legge per il caso di captazioni disposte all'estero ed effettuate nei confronti di persone il cui «indirizzo di comunicazione» è attivato in Italia. Non può sostenersi, infatti, che, nella specie, le operazioni non sarebbero state consentite «in un caso interno analogo», perché le stesse sono state disposte in ordine a reati per i quali la legge italiana prevede la possibilità di ricorrere a tale mezzo di ricerca della prova****, e, in particolare, per reati di associazione per delinquere finalizzata al traffico di sostanze stupefacenti e di traffico di sostanze stupefacenti".*

(…)

Invero, anche ad accogliere la qualificazione giuridica prospettata dai ricorrenti, i dati ottenuti mediante o.e.i.: a) non possono in alcun modo ritenersi risultati di intercettazioni disposte dall'autorità giudiziaria francese in modo generalizzato ed indiscriminato, ovvero in difetto di indizi concreti nei confronti degli utenti del sistema Sky-Ecc o comunque in violazione di «diritti fondamentali» o di principi costituzionali dell'ordinamento nazionale, o in contrasto con le garanzie

assicurate dall'art. 31 Direttiva 2014/41/UE, per le ragioni indicate nei §§ 18.5.1, 18.5.2, 18.5.3 e 18.5.4; b) sono stati acquisiti sulla base di richieste relative a persone nominativamente indicate, tra le quali i due attuali ricorrenti, in quel momento già tutte sottoposte ad indagini in Italia per i reati di partecipazione ad associazione per delinquere finalizzata al traffico internazionale di cocaina e di acquisto, detenzione, importazione e cessione di partite di tale tipo di droga.

Di conseguenza, nella vicenda in esame, non si pongono problemi di mancato rispetto delle condizioni previste dall'art. 6, paragrafo 1, lett. a) e b), Direttiva 2014/41/UE, o di interpretazione ed applicazione dell'art. 31 Direttiva cit.".

***

Queste, invece, le conclusioni delle **Sezioni Unite Gjuzi**: "*Ora, secondo i principi di diritto precedentemente enunciati,* ***l'emissione, da parte del pubblico ministero, di o.e.i. diretto ad ottenere il contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, non deve essere preceduta da autorizzazione del giudice italiano, perché tale autorizzazione non è richiesta, nell'ordinamento italiano, per l'acquisizione del contenuto di comunicazioni telefoniche già acquisite in altro procedimento, eventualmente anche se, a norma dell'art. 132 d.lgs. n. 196 del 2003, presso i gestori di servizi telefonici o telematici****.*

(…)

Per le ragioni precedentemente esposte, deve escludersi anche la necessità di formulare alla Corte di giustizia dell'Unione Europea i quesiti prospettati dalla difesa, ovvero di sollevare questione di legittimità costituzionale.

Invero, i dati oggetto dell'o.e.i. contestato: a) sono stati acquisiti dall'autorità francese nell'ambito di indagini concernenti un traffico internazionale di stupefacenti e sono stati successivamente trasmessi all'autorità italiana in relazione ad un procedimento concernente un'associazione per delinquere finalizzata al narcotraffico; b) sono stati richiesti ed ottenuti mediante o.e.i. dall'autorità giudiziaria italiana competente ad acquisirli «alle stesse condizioni in un caso interno analogo», in applicazione della disciplina sulla "circolazione" delle prove*.*

Di conseguenza, nella vicenda in esame, ***non si pongono problemi né di acquisizione di dati elettronici relativi al traffico, all'ubicazione o al contenuto di comunicazioni già in possesso della autorità di esecuzione, al di fuori di procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, né di mancato rispetto delle condizioni previste dall'art. 6 Direttiva 2014/41/UE***".

Conclusioni

La stagione apertasi con le operazioni EncroChat e SkyECC ha consegnato all'ordinamento italiano un patrimonio probatorio di dimensioni senza precedenti e, insieme, un complesso di questioni giuridiche di rilievo costituzionale, che la giurisprudenza nomofilattica del 2024 ha provveduto a sistemare in una cornice oggi sostanzialmente consolidata.

Al giudice delle indagini preliminari è chiesto di esercitare la funzione di vaglio con la consapevolezza che il dato criptato non è una prova diversa dalle altre, ma una prova che esige un di più di rigore nella verifica della provenienza, della catena di custodia, della

riferibilità soggettiva e del rispetto delle garanzie. Una prova, in altri termini, che richiede una particolare cura nella ricostruzione delle premesse di formazione, perché ai tradizionali problemi del giudice della cautela – quelli legati alla credibilità intrinseca delle fonti, alla coerenza dell'inferenza indiziaria, alla proporzionalità della misura – si aggiungono profili nuovi, legati all'opacità di parti significative del processo di formazione del dato, alla pluralità di soggetti istituzionali coinvolti nella sua estrazione e nella sua circolazione, alla difficoltà di una verifica indipendente che le tradizionali tecniche forensi consentivano in misura più piena.

È una funzione che si esercita, oggi più che mai, in dialogo costante con le Procure Distrettuali, con le Autorità Giudiziarie Europee e con il sistema sovranazionale di tutela dei diritti fondamentali. È in questo dialogo che si misura, in ultima analisi, la tenuta dell'equilibrio fra efficacia investigativa e legalità del processo: un equilibrio che la giurisprudenza del 2024 ha disegnato in modo nitido, ma che la prassi quotidiana è chiamata a riempire di contenuto, caso per caso, procedimento per procedimento.

Lo smantellamento delle grandi piattaforme *criminal by design* non ha determinato la sparizione del fenomeno, ma una sua riconfigurazione. Sul mercato si affacciano nuovi servizi (con tutta probabilità destinati a una nuova generazione di operazioni transnazionali di compromissione), accanto a piattaforme generaliste a sicurezza più rigorosa (Signal, Session, Matrix) che attraggono porzioni di utenza criminale qualificata. Si moltiplicano, parallelamente, i sistemi paralleli fondati su criptovalute, *mixer* e *dark net*, che pongono problemi non tanto di acquisizione del dato comunicativo quanto di tracciamento dei flussi economici e di identificazione degli intestatari.

Sul piano normativo, il prossimo ciclo passerà verosimilmente attraverso un consolidamento del quadro europeo. Il regolamento (UE) 2023/1543 sugli ordini europei di produzione e di conservazione delle prove elettroniche in materia penale, e la direttiva (UE) 2023/1544 che ne completa l'architettura sotto il profilo dell'individuazione di stabilimenti e rappresentanti legali nei diversi Stati membri, costituiscono il principale strumento di una cooperazione semplificata sulla prova elettronica, con un orizzonte applicativo che riguarda direttamente i fornitori di servizi di comunicazione e di *hosting*. Vanno altresì segnalati gli sviluppi in materia di cooperazione su captatori informatici, le riflessioni avviate in sede UE su uno statuto armonizzato dell'utilizzabilità delle prove transnazionali, e il dibattito – tuttora aperto – sull'introduzione di forme di accesso lecito ai contenuti cifrati che concilino le esigenze investigative con la tutela della sicurezza informatica del sistema (la cosiddetta *lawful access debate*).

Sul piano tecnologico, lo sviluppo della crittografia *post-quantum* e l'impiego di intelligenza artificiale nell'analisi dei grandi compendi di chat acquisite imporranno aggiornamenti tanto agli operatori del contrasto, quanto al giudice chiamato a valutarne i risultati. Per quanto attiene alla crittografia *post-quantum*, la prospettiva è quella di un consolidamento di nuovi algoritmi (in particolare quelli oggetto di standardizzazione presso il NIST statunitense) che renderanno strutturalmente più impegnativa qualunque azione di compromissione futura, costringendo le autorità di contrasto a un investimento crescente

nelle tecniche di accesso al dato a livello di terminale. Per quanto attiene all'intelligenza artificiale, lo sviluppo di strumenti di analisi semantica automatizzata dei grandi compendi di chat (anche multilingue) costituisce, a un tempo, un'opportunità per la gestione efficiente del materiale e una sfida sul piano della verificabilità del processo decisionale automatizzato: il giudice chiamato a valutare evidenze ottenute con il concorso di strumenti di intelligenza artificiale dovrà disporre di una documentazione sufficiente sul funzionamento dell'algoritmo, sulla qualità dei dati di addestramento e sul margine di errore del sistema.

In ogni scenario, il punto di equilibrio resterà quello fra l'effettività dell'azione di contrasto a una criminalità organizzata sempre più transnazionale e digitalmente attrezzata, da un lato, e il rispetto sostanziale dei diritti fondamentali coinvolti, dall'altro: un equilibrio che non è mai dato una volta per tutte, ma che deve essere ricostruito nella concreta dialettica processuale.

dott.ssa Giuseppina Laura Candito