



COMMENTO ALLE INFORMAZIONI PROVVISORIE DELLE SEZIONI UNITE IN RELAZIONE ALL'UTILIZZABILITÀ DELLE CHAT CRIPTATE ACQUISITE IN FRANCIA TRAMITE O.E.I.

Le Sezioni Unite della Corte di Cassazione hanno statuito che sono utilizzabili nei procedimenti penali italiani le chat criptate acquisite dai Pubblici Ministeri italiani attraverso lo strumento dell'ordine europeo d'indagine (OEI). Dalle informazioni provvisorie 3 e 4/2024 relative alle pronunce delle Sezioni Unite si possono trarre alcune conclusioni. In estrema sintesi, le Sezioni Unite hanno concluso che l'attività di acquisizione probatoria in questione andasse ricondotta alla disciplina di cui agli artt. 78 disp. att. c.p.p., 238 e 270 cpp. in applicazione della disciplina dell'acquisizione di prove provenienti da procedimenti stranieri (art. 78 disp. att. c.p.p. e 238 c.p.p.) e dell'utilizzazione delle intercettazioni in procedimenti diversi da quello di origine (art. 270 c.p.p.)

di **Vincenzo Scarlato**

IUS/16 - DIRITTO PROCESSUALE PENALE

Articolo divulgativo - ISSN 2421-7123

Direttore responsabile

Alessio Giaquinto

Publicato, Venerdì 19 Aprile 2024



Abstract ENG

United Sections of the Court of Cassation decided about encrypted chat's usability acquired through European order of investigation (O.E.I.) in France by Italian prosecutors in Italian criminal proceedings by European order of investigation. According to provisional information n. 3 - 4/2024, United Sections concluded that French investigative activity of evidentiary acquisition must be qualified according to the articles 78 disp. att. c.p.p., 238 and 270 c.p.p. in application of evidentiary acquisition from foreigner criminal proceeding (art. 78 disp. att. c.p.p. and 238 c.p.p.) and the usability of wiretraps in different proceeding compared to the original one (art. 270 c.p.p.)

Sommario: 1. Le informazioni provvisorie delle Sezioni Unite in relazione alla questione correlata all'utilizzabilità delle chat acquisite in Francia attraverso Ordine europeo d'indagine; 2. Premessa storica. L'indagine condotta dalle Autorità investigative straniere; 3. I primi arresti giurisprudenziali in relazione alle questioni di inutilizzabilità prospettate dalle difese. La qualificazione giuridica delle chat come documento informatico ex art. 234 bis c.p.p.; 4. La discontinuità determinata dalle sentenze di annullamento con rinvio della Sesta Sezione Penale e i dubbi interpretativi sulla disciplina normativa applicabile; 5. L'inquadramento delle chat criptate quale sequestro di corrispondenza telematica all'esito della sentenza n. 170/23 della Corte Costituzionale; 6. Gli orientamenti contrapposti e le ordinanze di rimessione alle Sezioni Unite della Suprema Corte delle ordinanze di rimessione; 7. La necessità di acquisizione dei provvedimenti autorizzativi e dei verbali delle operazioni relativi alle intercettazioni trasferite ex artt. 78 disp.att. c.p.p., 238, 270 c.p.p dal procedimento francese; 8. Conclusioni.

1. Le informazioni provvisorie delle Sezioni Unite in relazione alla questione correlata all'utilizzabilità delle chat acquisite in Francia attraverso Ordine europeo d'indagine

Le Sezioni Unite si sono pronunciate in relazione alla vexata quaestio correlata alla possibilità di utilizzare nei procedimenti penali interni le chat criptate acquisite dai Pubblici Ministeri italiani tramite Ordine Europeo d'Indagine.

Non si conoscono ancora le motivazioni della decisione adottata. Tuttavia, dalle informazioni provvisorie si può evincere sinteticamente che le Sezioni Unite hanno dato risposta affermativa al quesito relativo alla utilizzabilità dei risultati delle investigazioni condotte in procedimenti penali stranieri nei procedimenti penali interni.

Infatti, in ordine alla qualificazione giuridica da attribuire agli elementi di prova raccolti all'estero, la Suprema Corte ha aderito all'impostazione secondo cui le suddette modalità di acquisizione di elementi investigativi andrebbero ricondotte alla disciplina di cui agli artt. 78 disp. Att. C.p.p., 238 e 270 c.p.p.

Precisamente, per quanto concerne le conversazioni estratte ex post già intervenute e, dunque, non acquisite in tempo reale si ritenevano applicabili le disposizioni di cui agli artt. 78 disp. Att. C.p.p. e 238 c.p.p. Invece, per le conversazioni captate in fase dinamica, ovvero acquisite in tempo reale durante l'esecuzione delle operazioni di intercettazione, le Sezioni Unite hanno ricondotto tale acquisizione all'art. 270 c.p.p. che disciplina l'utilizzazione delle intercettazioni in altri procedimenti penali.

Il combinato disposto delle norme richiamate consentirebbe l'acquisizione nel quadro di un procedimento penale interno delle prove provenienti da procedimenti penali stranieri e, per quanto concerne gli elementi di prova da qualificare come intercettazioni, ne consentirebbe l'utilizzazione in procedimenti penali interni a condizione che si proceda nel quadro del procedimento ad quem italiano per un'ipotesi di reato per la quale è previsto l'arresto obbligatorio in flagranza ex art. 380 c.p.p.

In ogni caso, spetterebbe al Giudice nazionale un controllo successivo di legittimità dell'attività svolta all'estero verificando in concreto "il rispetto dei diritti fondamentali, comprensivi del diritto di difesa e della garanzia di un equo processo".

2. Premessa storica. L'indagine condotta dalle Autorità investigative straniere

Va premesso che nell'ambito di inchieste coordinate tra Belgio, Olanda e Francia, le Autorità investigative dei suddetti Stati sono riuscite a violare la piattaforma del sistema criptato "SkyEcc", ottenendo, attraverso l'intercettazione statica e dinamica complessiva dei server, tutti i flussi di comunicazioni transitati e transitanti sui dispositivi degli utilizzatori della suddetta piattaforma criptata.

Essa consentiva agli utenti di scambiare chat e chiamate senza la possibilità di essere intercettati attraverso gli ordinari strumenti di captazione.

All'esito delle suddette operazioni investigative svolte all'estero, i Pubblici Ministeri italiani chiedevano la trasmissione delle chat criptate acquisite attraverso tali modalità. Tali richieste venivano inoltrate allo Stato estero attraverso lo strumento dell'Ordine Europe d'indagine (O.E.I.). In particolare, l'O.E.I. aveva ad oggetto l'acquisizione ex post delle chat riconducibili a soggetti determinati ovvero a soggetti ancora indeterminati ma

dei quali veniva individuato esclusivamente il “nickname” abbinato all’utenza SkyEcc sottoposta a sequestro e contestuale intercettazione dei flussi di comunicazione.

Attraverso tale strumento venivano dunque richiesti dai PM italiani elementi di prova già detenuti dall’Autorità investigativa straniera. Sulla base degli elementi investigativi acquisiti attraverso tali modalità venivano richieste ed accolte numerose richieste di provvedimenti cautelari personali e reali integralmente imperniate sui contenuti delle chat acquisite dalle Autorità investigative nei vari Stati dell’Unione Europea.

3. I primi arresti giurisprudenziali in relazione alle questioni di inutilizzabilità prospettate dalle difese. La qualificazione giuridica delle chat come documento informatico ex art. 234 bis c.p.p.

La giurisprudenza nazionale ha immediatamente aderito all’impostazione secondo cui l’acquisizione delle prove già in possesso dell’A.G. di uno Stato straniero va sempre considerata legittima, trattandosi di acquisizione di dati informatici già detenuti legittimamente dal legittimo titolare ovvero lo Stato francese (1).

La Suprema Corte, nel rigettare le questioni prospettate dalle difese in ordine alla (il)legittimità dell’attività investigativa svolta all’estero, precisava che nei procedimenti penali interni risultava sottratto al Giudice nazionale il sindacato relativo alla legittimità della prova acquisita all’estero (2). In ogni caso, le modalità di acquisizione di tali conversazioni criptate presentavano una pluralità di profili di criticità.

Tali criticità venivano evidenziate dalle difese in una pluralità di ricorsi imperniati essenzialmente sull’inutilizzabilità delle chat criptate acquisite in Francia sulla scorta dell’assenza di provvedimenti autorizzativi basati sui presupposti normativi previsti in tema di intercettazioni ex artt. 266 e ss. c.p.p.

Si censurava l’illegittimità dei provvedimenti emessi dai giudici francesi atteso che venivano autorizzate intercettazioni verso un numero indeterminato di soggetti in assenza di elementi preesistenti di natura indiziaria e di indispensabilità ai fini della prosecuzione delle indagini nonché l’assenza totale di motivazione specifica in merito al collegamento tra l’indagine in corso e le singole utenze abbinare agli account “skyEcc”.

Veniva poi dedotta l’illegittimità dell’attività investigativa svolta in Francia conseguente a presunte lesioni del diritto di difesa derivanti dall’omessa comunicazione delle modalità di decriptazione delle conversazioni ab origine criptate in quanto coperte da segreto di Stato. Infine, veniva anche eccepita l’incompetenza del PM italiano in materia di

emissione dell'O.E.I. con conseguente inutilizzabilità della prova illegittimamente acquisita.

In sintesi, ad avviso delle difese, allorquando la prova da acquisire all'estero dovesse essere ricondotta alla disciplina delle intercettazioni, sarebbe stato necessario un provvedimento autorizzativo del Giudice per le indagini preliminari che autorizzasse tale acquisizione considerata la doppia riserva di legge e di giurisdizione di cui all'art. 15 Cost. in tema di riservatezza delle comunicazioni secondo cui la corrispondenza può essere violata solo su atto motivato dell'Autorità giudiziaria con le garanzie stabilite dalla legge.

Tale necessità deriverebbe dal fatto che il PM non avrebbe potuto ordinare le intercettazioni in un caso interno analogo in assenza di un qualsiasi provvedimento che verificasse in concreto l'esistenza di un quadro di gravità (ovvero sufficienza) indiziaria e di indispensabilità (ovvero necessità) dell'esecuzione delle operazioni ai fini della prosecuzione delle indagini.

Bisogna chiarire subito che la Francia, in relazione alle modalità di acquisizione dei dati investigativi consistenti nelle chat criptate sopra richiamate, opponeva il segreto di Stato (3).

Non veniva consentita dunque alle difese la possibilità di censurare le modalità di acquisizione delle conversazioni riconducibili ai soggetti coinvolti atteso che non veniva reso disponibile né l'algoritmo per la decifrazione delle suddette chat né il sistema informatico attraverso cui si era pervenuti alla captazione delle stringhe informatiche originarie, solo successivamente decriptate grazie all'individuazione della chiave di decifrazione delle stesse.

L'ignoranza incolpevole delle difese in relazione a tali modalità di acquisizione e di decifrazione ha condizionato pesantemente il diritto di difesa di tutti gli soggetti coinvolti in tale operazione di mastodontica captazione. Il pregiudizio arrecato alle garanzie difensive risultava ancor più evidente se si considera quanto ribadito dalla Suprema Corte in ordine alla presunzione di legittimità dell'attività investigativa svolta all'estero (4).

Ne consegue che l'imputato si ritrovava ristretto in una "morsa di ferro" poiché, da un lato, si presumeva legittima l'attività investigativa svolta all'estero e, dall'altro, si opponeva il segreto di Stato in relazione alle modalità di estrinsecazione di tale attività impedendo di fatto ogni controllo o censura in ordine alla legittimità delle suddette operazioni investigative. Il dubbio che si pone l'interprete è il seguente: come si può censurare un'attività investigativa svolta all'estero (che si presume legittima) se non si

conosce il *modus operandi* seguito dall'Autorità inquirente e viene opposto il segreto di Stato sulle modalità di estrinsecazione dell'attività investigativa e di acquisizione del dato indiziario?

La Corte di cassazione tra il 2022 e il 2023 si era già pronunciata più volte in ordine alla utilizzabilità dei dati estrapolati dalle piattaforme “EncroChat” e “Sky-ecc” acquisiti attraverso O.E.I. dalla Francia nel quadro di una moltitudine di ricorsi presentati avverso provvedimenti applicativi di misure cautelari.

Le pronunce in questione avevano univocamente ritenuto che la messaggistica criptata intercettata, 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. (5).

In tali pronunce, veniva superata l'eccezione di inutilizzabilità del materiale proveniente dal procedimento francese acquisito tramite lo strumento interno dell'O.E.I. 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) trattandosi 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 decriptazione 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.

4. La discontinuità determinata dalle sentenze di annullamento con rinvio della Sesta Sezione Penale e i dubbi interpretativi sulla disciplina normativa applicabile

In un secondo momento sono intervenute le sentenze della VI Sezione Penale n. 44154 e 44155 del 26.10.2023 (6). Queste ultime, annullando con rinvio due ordinanze cautelari emesse dal Tribunale del Riesame di Milano e di Reggio Calabria, hanno segnato un momento di discontinuità nel quadro del dibattito giurisprudenziale relativo

all'utilizzabilità interna delle prove raccolte nel procedimento francese e alla corretta qualificazione giuridica da attribuire alle suddette modalità di acquisizione probatoria.

Infatti, con tali pronunce, la Suprema Corte ha escluso l'operatività dell'art. 234-bis c.p.p., ritenendola applicabile solo in caso di acquisizione di documenti e dati informatici "dematerializzati", cioè preesistenti rispetto all'inizio delle investigazioni condotte dall'autorità giudiziaria francese ovvero che erano stati formati al di fuori di quelle investigazioni: nei casi in esame, di contro, gli elementi sono stati acquisiti nel quadro di 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 perquisizione e sequestri, in specie nell'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 del d.lgs. 196/2003 come modificato dal d.lgs. 132/2021 nonché 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. 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.

5. L'inquadramento delle chat criptate quale sequestro di corrispondenza telematica all'esito della sentenza n. 170/23 della Corte costituzionale

Una successiva sentenza (7) ha perorato un diverso orientamento. In particolare, la qualificazione giuridica dei dati raccolti all'estero veniva ricondotta al concetto di corrispondenza telematica.

In quanto tale, in caso di sequestro probatorio eseguito da parte del Pubblico ministero, non vi sarebbe la necessità di una preventiva autorizzazione del giudice, ma sarebbe sufficiente soltanto il provvedimento motivato del PM.

Nella suddetta pronuncia veniva valorizzato l'orientamento perorato dalla Corte Costituzionale che, nella recente sentenza n. 170/2023 (8) relativa ad un'ipotesi di sequestro probatorio di corrispondenza riconducibile ad un parlamentare, ha affermato che la messaggistica conservata acquisita ex post non ha natura di generico documento, bensì mantiene il suo carattere di "corrispondenza", dovendosi ritenere permanere l'interesse alla riservatezza «almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento storico». Pertanto, partendo da tale presupposto, la Corte concludeva che la messaggistica acquisita dalle Autorità francesi, costituendo del pari registrazione di conversazioni già avvenute e, quindi, di dati "statici", è assimilabile alla corrispondenza, la quale non necessita di un provvedimento del giudice, potendo essere acquisita con decreto motivato di sequestro probatorio disposto dal pubblico ministero.

6. Gli orientamenti contrapposti e le ordinanze di rimessione alle Sezioni Unite della Suprema Corte delle ordinanze di rimessione

Preso atto dell'esistenza di diversi orientamenti giurisprudenziali in ordine alla disciplina corretta da applicare al caso dell'acquisizione nei procedimenti penali interni delle chat criptate dall'estero, la Terza Sezione Penale con l'ordinanza n. 47998 (9) del 30 novembre 2023 e la Sesta Sezione Penale con l'ordinanza n. 2329 (10) depositata il 18 gennaio 2024 hanno ritenuto di rimettere alle Sezioni Unite la risoluzione delle questioni di diritto prospettate nei ricorsi correlate alle modalità di acquisizione delle chat criptate e alla loro utilizzabilità interna.

Le Sezioni Unite hanno aderito all'impostazione già seguita dalla giurisprudenza precedente ritenendo legittima l'attività svolta all'estero e utilizzabile il materiale investigativo acquisito tramite O.E.I. In relazione alle disposizioni interne applicabili all'acquisizione probatoria censurata, sembrerebbe che le Sezioni Unite abbiano ricondotto l'acquisizione probatoria delle chat criptate acquisite in Francia alla disciplina di cui agli artt. 78 disp. att. c.p.p e 238 c.p.p. Inoltre, dall'informazione provvisoria si evince che le Sezioni Unite avrebbero confermato altresì l'applicabilità dell'art. 270 c.p.p. nelle ipotesi di acquisizione delle chat criptate sviluppatesi nella fase dinamica.

Attraverso tale impostazione, si è legittimata l'utilizzazione delle intercettazioni eseguite nell'originario procedimento francese in procedimenti penali italiani interni evidentemente diversi da quello nell'ambito del quale erano state autorizzate. È evidente che tale utilizzazione dovrà considerarsi circoscritta alle sole ipotesi previste dall'art. 270 c.p.p. (ovvero alle ipotesi di reati per i quali è previsto l'arresto obbligatorio in flagranza ex art. 380 c.p.p.).

7. La necessità di acquisizione dei provvedimenti autorizzativi e dei verbali delle operazioni relativi alle intercettazioni trasferite ex artt. 78 disp.att. c.p.p., 238, 270 c.p.p dal procedimento francese

Infine, si segnala l'ultima pronuncia della Suprema Corte (11) in relazione alla questione correlata all'utilizzabilità delle chat criptate trasferite dal procedimento francese. Nel ricorso sottoposto al vaglio della Suprema Corte, la difesa lamentava l'inutilizzabilità delle chat criptate acquisite con O.E.I. alla luce del fatto che il PM aveva omesso di allegare i provvedimenti autorizzativi emessi nel procedimento francese.

La difesa evidenziava altresì che la documentazione richiesta e, non depositata dal PM procedente, aveva determinato una lesione del diritto di difesa conseguente all'impossibilità di esaminare le modalità di acquisizione delle chat criptate. Precisamente, veniva evidenziato che l'assenza dei provvedimenti autorizzativi e dei verbali relativi al compimento delle operazioni, non aveva consentito alle difese di verificare le modalità di acquisizione e decifrazione dei flussi telematici.

Inoltre, attraverso l'omessa produzione della documentazione richiesta dalla difesa, veniva di fatto impedita la verifica ex post del preventivo controllo dell'autorità giudiziaria sempre necessario rientrando la messaggistica acquisita nella nozione di corrispondenza se non di dati acquisiti mediante attività di intercettazione.

Per tale ragione, l'autorità giudiziaria francese, in sede di esecuzione dell'ordine europeo di indagine, avrebbe dovuto trasmettere anche i verbali attestanti le modalità di acquisizione dei dati informatici e di svolgimento delle operazioni di decriptazione e trascrizione degli stessi per consentire alla difesa il controllo sul rispetto dei principi fondamentali e delle norme inderogabili del nostro ordinamento a cominciare dal diritto alla formazione della prova in contraddittorio.

Nello specifico la difesa argomentava affermando che l'omessa allegazione della documentazione tempestivamente richiesta non aveva consentito di accertare se il messaggio crittografato era stato acquisito mediante l'intercettazione del flusso telematico, mediante inoculazione di un captatore informatico ovvero mediante la acquisizione del documento informatico conservato nel server a comunicazione esaurita. Ciò, ad avviso del ricorrente, avrebbe determinato un vulnus ai diritti dell'indagato in quanto avrebbe determinato un'incertezza sulla disciplina applicabile alla prova acquisita all'estero. Incertezza superabile solo attraverso l'acquisizione dei provvedimenti autorizzativi e dei verbali delle operazioni eseguite in Francia che, secondo la difesa, avrebbe consentito di qualificare in modo corretto le modalità di acquisizione della prova

consentendo, in tal modo, l'individuazione della disciplina positiva interna applicabile al caso concreto.

Ne consegue che l'acquisizione dei risultati andrebbe considerata legittima solo nel caso in cui risultino rispettati i requisiti previsti dall'art. 270 cod. proc. pen., mentre, se l'acquisizione è avvenuta mediante la copiatura del dato informatico conservato nel server o la perquisizione del sistema informatico o telematico, andranno applicate le regole in materia di copia forense e di garanzia della genuinità del dato informatico.

Alla luce dei rilievi difensivi, la Suprema Corte riteneva fondato il ricorso della difesa e, dunque, annullava l'ordinanza impugnata con rinvio al Tribunale del Riesame. Infatti, la Prima Sezione Penale, richiamando le informazioni provvisorie delle Sezioni Unite, condivideva le prospettazioni difensive in relazione alla necessità di acquisizione della documentazione investigativa proveniente dal procedimento d'origine.

Nella sentenza, infatti, si affermava espressamente che il Tribunale del riesame aveva commesso un errore nel ritenere irrilevante la valutazione relativa alle modalità di acquisizione del materiale proveniente dalla Francia. Infatti, come correttamente sollecitato la difesa, sarebbe stato necessario acquisire tale documentazione al fine di stabilire la disciplina interna applicabile a tale modalità di acquisizione probatoria.

Pertanto, ritenuto assorbente il motivo di impugnazione, la Suprema Corte concludeva per l'annullamento con rinvio al Tribunale del Riesame affinché, previa acquisizione della documentazione attestante le modalità di acquisizione del materiale indiziario proveniente dalla Francia, determinasse la disciplina applicabile.

Precisamente, in caso di attività di acquisizione probatoria riconducibile alla disciplina del sequestro, troveranno applicazione le disposizioni in materia di copia forense dei dispositivi informatici. Diversamente, nel caso in cui si tratti di esiti di attività di intercettazione dei flussi di comunicazione, ovvero di intercettazione a mezzo captatore informatico, bisognerà applicare le disposizioni interne che regolano l'utilizzo di tali strumenti di ricerca della prova dettate dagli artt. 266 bis e ss. c.p.p.

8. Conclusioni

Ad avviso di chi scrive, la pronuncia in questione bilancia in parte l'irrimediabile vulnus al diritto di difesa determinato dall'impossibilità di fatto di eccepire eventuali illegittimità delle acquisizioni probatorie eseguite in Francia con la necessità di prevedere un controllo giurisdizionale interno dell'attività investigativa svolta all'estero.

Al fine di rendere effettivo il vaglio giurisdizionale di legalità sostanziale dell'attività investigativa svolta all'estero, l'auspicio è che non ci si limiti soltanto ad una acquisizione formale della documentazione a supporto delle indagini.

Dopotutto, una verifica della legittimità sostanziale condotta secondo i canoni del diritto italiano, ovvero, un vaglio preventivo giurisdizionale in relazione all'utilizzabilità nel procedimento interno della prova acquisita all'estero risulterebbe anche in armonia anche con i principi costituzionali ex artt. 2, 3, 14, 15, 24, 111 e 113 Cost. e sovranazionali artt. 1, 5, 6 CEDU. In definitiva, le criticità evidenziate risultano ancora lontane da un'adeguata risoluzione.

I temi sono estremamente rilevanti ed attengono all'effettività delle garanzie difensive interne in relazione alla pervasività degli strumenti investigativi di ricerca della prova attivabili da uno Stato estero. Va infatti rammentato che lo strumento di ricerca della prova attivato in Francia non si limita ad incanalare tutti i dati statici preesistenti nel dispositivo, ma è in grado anche di captare in fase dinamica ogni singola attività del dispositivo oggetto di intrusione informatica.

Dunque, se può essere sufficiente il provvedimento del PM per operare il sequestro della corrispondenza intesa staticamente, ciò non è sufficiente in relazione a tutti i dati acquisiti in fase dinamica. Inoltre, in relazione ai provvedimenti autorizzativi dei giudici francesi, pur aderendo all'impostazione prospettata dal P.G. nella requisitoria scritta depositata alle Sezioni Unite secondo cui i provvedimenti di autorizzazione all'intercettazione del server erano motivati oltre lo standard motivazionale richiesto dall'ordinamento nazionale (12), risulta comunque la grave carenza strutturale degli stessi rispetto al collegamento con le utenze determinate da captare.

La Suprema Corte ha affermato ripetutamente che in tema di intercettazioni telefoniche, la motivazione del decreto autorizzativo deve necessariamente dar conto delle ragioni che impongono l'intercettazione di una determinata utenza telefonica che fa capo ad una specifica persona e, perciò, non può omettere di indicare il collegamento tra l'indagine in corso e la medesima persona, affinché possa essere verificata, alla luce del complessivo contenuto informativo e argomentativo del provvedimento, la sua adeguatezza rispetto alla funzione di garanzia prescritta dall'art. 15, comma 2 Cost (13).

Infatti, aderendo all'impostazione del P.G. risulterebbero legittimamente eseguite tutte le captazioni operate nei confronti di una serie indefinita di soggetti per i quali non sussisteva alcun elemento preesistente che consentisse il ricorso alle intercettazioni secondo le disposizioni del diritto interno.

Così ragionando si porrebbe a conseguenze aberranti e verrebbe completamente eluso il principio costituzionale di inviolabilità della corrispondenza e la doppia riserva di legge e di giurisdizione ex art. 15 Cost. In altri termini, l'art. 15 della Costituzione, fissando l'inviolabilità della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione, ha previsto al secondo comma che la loro limitazione possa avvenire soltanto per atto motivato dell'autorità giudiziaria e con le garanzie stabilite dalla legge. Ne consegue che l'affermazione dell'inviolabilità risulta strettamente connessa con il sistema di garanzie successivamente disposto, tanto da non poter ritenere che la clausola dell'inviolabilità assuma un significato meramente retorico (14).

Pertanto, bisogna sottolineare come nel caso di attivazione da parte di Paesi stranieri di strumenti di ricerca della prova nei confronti di soggetti che si trovano in Italia, questi non solo non risponderanno alla legge italiana in relazione ai requisiti richiesti per l'attivazione e i limiti all'utilizzazione processuale di quanto acquisito, ma soprattutto risulteranno sottratti al controllo giurisdizionale interno relativo al rispetto delle garanzie difensive stabilite dall'ordinamento processuale italiano. Si aggiunge come in Francia i decreti autorizzativi delle intercettazioni sono provvedimenti sostanzialmente amministrativi (15), privi di motivazione e, soprattutto, non sono impugnabili (cfr. art. 100 – 2 Code de Procédure Pénal: “La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours”) a differenza del sistema interno che consente di rilevare anche d'ufficio in ogni stato e grado l'inutilizzabilità delle intercettazioni, persino all'esito di giudizio di rinvio a seguito di sentenza di annullamento con rinvio della Suprema Corte, trattandosi di c.d. inutilizzabilità patologica (cfr. Cass. Pen., Sez. III, n. 15828/14) (16).

La difesa dei diritti non può essere sacrificata in favore della necessità di conservazione della prova di segno colpevolista. L'enfaticizzazione delle esigenze investigative è un argomento inconferente soprattutto se si considera che gran parte delle intercettazioni venivano eseguite in assenza di un quadro preesistente di gravità indiziaria.

In ogni caso, la base indiziaria arguibile dai provvedimenti del Giudice istruttore francese poteva al massimo riguardare un numero estremamente limitato di soggetti e non può certamente giustificare l'acquisizione massiva dei dati freddi e l'intercettazione telematica dinamica di oltre 70.000 soggetti indeterminati per il semplice fatto che siano utilizzatori della piattaforma skyEcc. La mera utilizzazione del sistema di comunicazione criptata è una circostanza che non può seriamente elevarsi ad indizio (neppure sufficiente) di reato. Comunque, la motivazione del decreto autorizzativo dovrebbe dare sempre conto del collegamento tra l'utenza da intercettare e l'indagine in corso.

Nel quadro del presente procedimento non v'è alcuna motivazione specifica e, certamente

non si potrà condividere l'impostazione in forza della quale veniva accreditata la necessità di procedere alla captazione di tutti i flussi di comunicazione di ogni singola utenza utilizzatrice del sistema di comunicazione "skyECC". Ciò renderebbe il mero utilizzo di una piattaforma di comunicazione non vietata dalla legge un elemento di sospetto tanto forte da determinare la necessità di intercettare e acquisire i dati massivi di oltre 70.000 soggetti indeterminati.

Va aggiunto un ulteriore profilo di inutilizzabilità che non è stato ancora sottoposto al vaglio della Suprema Corte e che si ritiene di grande rilevanza. Nello specifico, si intende evidenziare la violazione dell'art. 271 c.p.p. in relazione all'art. 267 comma 3 c.p.p. e all'art. 13 comma 2 D.L. n. 152/91. Infatti, l'art. 13 comma 2 D.L. n. 152/91 prevede che: "Nei casi di cui al comma 1, la durata delle operazioni non può superare i quaranta giorni, ma può essere prorogata dal giudice con decreto motivato per periodi successivi di venti giorni, qualora permangano i presupposti indicati nel comma 1. Nei casi di urgenza, alla proroga provvede direttamente il pubblico ministero; in tal caso si osservano le disposizioni del comma 2 dell'articolo 267 del codice di procedura penale". Nel caso di specie, il provvedimento del giudice istruttore francese autorizzava l'intercettazione del server per mesi 4.

È evidente che tutto il materiale intercettato successivamente ai 40 giorni dall'autorizzazione del giudice istruttore andrà considerato inutilizzabile ai sensi dell'art. 271 c.p.p. attesa la palese violazione dell'art. 267 comma 3 c.p.p. che prevede la necessità di proroga ogni 15 giorni laddove permangano i presupposti che hanno condotto all'autorizzazione (ovvero dopo 40 giorni con successive proroghe di 20 giorni nei casi disciplinati dall'art. 13 D.L. n. 152/91). L'elusione della normativa nazionale in ordine alla necessità di un controllo giurisdizionale circoscritto a determinate scansioni temporali rappresenta un argomento che dovrebbe superare la presunzione di legittimità dell'attività investigativa svolta all'estero. Verrebbe infatti prospettata una effettiva lesione del diritto di difesa conseguente all'assenza di un controllo giurisdizionale che sarebbe previsto in un caso interno analogo.

Ciò determinerebbe un'ingiustificabile estensione della durata delle operazioni di intercettazione ai danni di un cittadino italiano in assenza di controllo giurisdizionale con conseguente vulnus al principio di inviolabilità della corrispondenza tutelato dall'art. 15 Cost.

Infatti, la disciplina dell'inutilizzabilità di cui agli artt. 254,267,270 e 271 va ricondotta alla tutela costituzionale apprestata alle comunicazioni dall'art.15 della Costituzione. Il diritto alla riservatezza della corrispondenza e di ogni mezzo di comunicazione non è che un aspetto essenziale della stessa inviolabilità della persona, e perciò è direttamente

riconducibile nella categoria dei diritti inviolabili dell'uomo (17).

In conclusione, è possibile affermare che lo strumento di ricerca della prova attivato in Francia può anche risultare giustificabile nell'ottica della difesa nazionale e della prevenzione e repressione di fenomeni di criminalità organizzata e terroristica.

Tuttavia, tale utilizzo andrebbe limitato alla sola acquisizione dei dati indiziari per finalità investigative e di prevenzione, dovendosi negare in radice la possibilità di utilizzazione ex post della prova acquisita attraverso un'operazione di intrusione informatica indiscriminata e massiva come quella eseguita in Francia a fortiori se le conversazioni intercettate si sono sviluppate integralmente al di fuori dei confini francesi.

Peraltro, in virtù dell'irrelevanza della c.d. inutilizzabilità derivata, gli elementi indiziari acquisiti attraverso tale operazione d'intrusione informatica avrebbero potuto pacificamente costituire la base indiziaria legittima per operazioni investigative legittimamente autorizzate. Ciò in virtù del principio secondo cui, in tema di inutilizzabilità, non si estende la trasmissibilità del vizio agli atti consecutivi a quello dichiarato nullo. (18)

Tali profili di illegittimità dei provvedimenti autorizzatori francesi ovvero dei provvedimenti con i quali veniva richiesta la trasmissione del materiale captato in Francia verranno verosimilmente superati dalle considerazioni sviluppate dalla Procura Generale presso la Suprema Corte che ha affermato come sia sostanzialmente impossibile intercettare il sistema criptato "skyEcc" attraverso modalità diverse da quelle eseguite in Francia.

In sintesi, ad avviso del P.G., un'interpretazione che neghi cittadinanza nei procedimenti penali italiani agli elementi investigativi acquisiti attraverso O.E.I. in Francia determinerebbe un'immunità (19) per gli utilizzatori del sistema criptato dalla possibilità di poter essere intercettati. Inoltre, tale immunità verrebbe garantita a soggetti quali gli utilizzatori dei sistemi criptati che vengono utilizzati prevalentemente per finalità criminali ovvero per eludere eventuali investigazioni.

Non risulta in ogni caso alcun tipo di controllo né a monte né a valle sulla proporzionalità tra le necessità di investigare in relazione a traffici internazionali di stupefacenti e l'opportunità di intercettare decine di migliaia di soggetti che con quella specifica investigazione nulla hanno a che vedere. In conclusione, risulta abbastanza evidente che la ragion di Stato (di Polizia) ha prevalso, almeno per adesso, con un pregiudizio evidente sulle garanzie costituzionali interne dei cittadini e sulla tenuta dello Stato di diritto rispetto ad influenze indebite di altri Stati non solo sul piano politico ma anche sul piano

giudiziario.

L'auspicio è che la Corte costituzionale italiana possa intervenire quanto prima affinché venga riaffermata la supremazia dello Stato di diritto. Ciò risulta necessario soprattutto se si considera che stiamo vivendo in un periodo storico in cui l'influenza politica di altri Stati e il potere della tecnologia rischiano di relegare gli spazi di libertà a margini inaccettabili. Tuttavia, le esigenze di affidabilità e di coordinamento del sistema interno con gli altri sistemi dei Paesi dell'UE inducono lo scrivente a ritenere che la Corte Costituzionale italiana si allineerà verosimilmente alle decisioni già adottate dalle Corti Costituzionali europee che hanno già dato risposta affermativa al quesito relativo alla legittimità dell'attività investigativa condotta in Francia (20).

In ogni caso, nei procedimenti penali interni si ritiene opportuno quantomeno bilanciare l'assenza di contraddittorio in ordine al materiale acquisito rappresentato dalle chat criptate con la necessità di riscontri estrinseci rispetto al contenuto delle conversazioni criptate acquisite.

Infatti, il giudice di merito dovrebbe andare alla ricerca di un adeguato grado di conferma dei fatti rappresentati dalle comunicazioni nel rimanente materiale probatorio, non potendo ritenere legittime decisioni integralmente impregnate sul contenuto di chat criptate acquisite all'estero talvolta a distanza di un notevole lasso di tempo. Tale esigenza, non dettata da una logica meramente garantista, non avrebbe neppure bisogno di un'apposita statuizione legislativa, risultando connaturata alla necessità di osservare lo standard dell'al di là di ogni ragionevole dubbio ex art. 533 comma 1 c.p.p. (21).

Infine, va aggiunto che in relazione alle intercettazioni a "bersaglio indeterminato" adottate nell'inchiesta francese, la Corte Regionale di Berlino ha sollevato, al riguardo, rinvio pregiudiziale alla Corte di Giustizia dell'Unione Europea, in causa C-670/22, con riferimento alla interpretazione dell'art. 6, paragrafi 1 e 2, lettere a) e b) della direttiva 2014/41/UE, la cui decisione è stata riservata (22).

In particolare, al punto 2. a.) viene rimesso alla Corte di Giustizia il seguente quesito : "Se l'articolo 6, paragrafo 1, lettera a), della direttiva 2014/41 osti a un OEI volto al trasferimento di dati già disponibili nello Stato di esecuzione (la Francia) derivanti da un'intercettazione di telecomunicazioni — in particolare, dati relativi al traffico e all'ubicazione, nonché registrazioni dei contenuti delle comunicazioni — qualora, in primo luogo, l'intercettazione effettuata dallo Stato di esecuzione riguardi tutti gli utenti di un determinato indirizzo di comunicazione, in secondo luogo, venga richiesto, tramite l'OEI, il trasferimento dei dati relativi a tutti gli indirizzi utilizzati sul territorio dello Stato di emissione e, in terzo luogo, non vi fossero indizi concreti della commissione di gravi

reati da parte di detti singoli utenti al momento in cui è stata disposta ed eseguita la misura di intercettazione né al momento dell'emissione dell'O.E.I.”.

L' Avvocato Generale Capèta, nelle proprie conclusioni formulate alla Corte di Giustizia in relazione alla suddetta causa (23), ha ribadito che allo Stato di emissione dell'O.E.I. è riservata una valutazione di ammissibilità della prova acquisita in violazione del diritto comunitario e che, tale valutazione, deve essere compiuta entro i canoni del diritto nazionale. In ogni caso, nelle conclusioni rassegnate, l'Avvocato generale Tamara Capèta ricorda che un O.E.I. può essere emesso soltanto se l'atto investigativo in esso richiesto avrebbe potuto essere emesso alle stesse condizioni in un caso interno analogo.

Pur approdando alla conclusione che il trasferimento di prove già acquisite renda irrilevante l'accertamento sulla tipologia di atto investigativo eseguito all'estero, l'Avvocato generale conferma la necessità di sottoporre al vaglio di legittimità interno il materiale probatorio acquisito dal procedimento francese.

Tuttavia, rispetto al requisito dell'ammissibilità alle stesse condizioni in un caso interno analogo, si ribadisce l'impossibilità di ritenere legittima l'operazione di intercettazione massiva condotta in Francia ai sensi dell'ordinamento processuale interno. Infatti, pur rilevando l'assenza di precedenti indagini interne eseguite attraverso la realizzazione di un'intercettazione internazionale massiva di una piattaforma informatica in uso a decine di migliaia di utenti di svariati Stati, può pacificamente concludersi per la non conformità, rispetto ai canoni previsti dal diritto interno, di un provvedimento che autorizzi indiscriminatamente la captazione di migliaia di utenze indeterminate senza sufficienti elementi che giustificano il ricorso e la prosecuzione delle operazioni.

La Corte di giustizia, peraltro, aveva già ripetutamente affermato che le modalità di tutela dei diritti operanti a livello eurounitario non dovrebbero essere meno favorevoli rispetto a quelle relative a situazioni analoghe assoggettate al diritto interno, evitando che informazioni ed elementi di prova ottenuti in modo illegittimo rechino indebitamente pregiudizio a una persona sospettata di avere commesso reati (24).

In definitiva, nell'attesa della decisione della Corte di Giustizia in relazione al rinvio pregiudiziale promosso dallo Stato tedesco, bisogna prendere atto che la giurisprudenza nazionale delle Sezioni Unite ha avallato, allo stato, la legittimità dell'attività investigativa eseguita in Francia. Resta comunque l'auspicio che la giurisprudenza sovranazionale possa ripristinare la sovranità territoriale dei singoli Stati tutelando la riservatezza delle comunicazioni dei cittadini da indebite operazioni di aggressione informatica che potrebbero attuare gli Stati stranieri.

Infatti, va rammentato come, nel caso di specie, le conversazioni captate in Francia si sono sviluppate quasi integralmente al di fuori del territorio francese. Pertanto, l'intercettazione dei flussi di comunicazione riconducibili a dispositivi in uso a cittadini stranieri, avrebbe necessitato della richiesta di assistenza degli Stati esteri nei cui confini si sviluppavano le captazioni. Non potrà al riguardo obiettarsi che le operazioni sono state eseguite interamente in Francia considerato che, per pacifica ammissione della stessa A.G. francese, si è proceduto all'installazione di captatori informatici su tutte le utenze skyECC indistintamente. In effetti, le Autorità francesi hanno chiarito che, nel corso delle indagini, al fine di pervenire alla decriptazione delle conversazioni, è stato necessario inoculare un trojan nei singoli criptofonini per apprendere la chiave di cifratura delle conversazioni.

Tale operazione di intrusione informatica è avvenuta in relazione ad ogni singolo criptofonino con la consapevolezza che gli utenti oggetto di tale aggressione informatica erano cittadini di altri Stati e che le conversazioni ricondotte a questi ultimi avvenivano nei confini dei suddetti Stati. Nondimeno, gli investigatori, prima di procedere con l'installazione generalizzata dei trojan, avevano già avuto modo di individuare i c.d. "metadati" riconducibili ai singoli criptofonini (25).

In questo modo, avendo conoscenza dei dati GPS e del codice IMEI relativi alla singola utenza, l'A.G. francese avrebbe potuto richiedere agli Stati di residenza degli utilizzatori delle utenze un'autorizzazione ad hoc al fine di eseguire le operazioni di captazione all'interno dei rispettivi confini nazionali. Inoltre, gli Stati interessati avrebbero potuto richiedere alla stessa A.G. francese, attraverso l'emissione di un O.E.I., l'esecuzione delle operazioni di captazione dei flussi di comunicazioni transanti sui dispositivi skyECC in uso ai propri cittadini.

A tal proposito si evidenzia come, già dall'avvio delle investigazioni intraprese sulla piattaforma skyECC dal Belgio, le Autorità di tale Stato erano riuscite a circoscrivere gli utilizzatori delle utenze all'interno dei confini nazionali e, addirittura all'interno della specifica città di Anversa. Le autorità belghe e olandesi riuscivano addirittura a quantificare gli utilizzatori mondiali di skyECC individuando un numero complessivo di circa di 68.000 utenti. Per quanto riguarda il numero degli utilizzatori totali stimati in Belgio, venivano quantificati in circa 8.000 utilizzatori. (26)

In conclusione, nell'attesa del deposito delle motivazioni delle Sezioni Unite, restano una serie di questioni irrisolte. In ogni caso, appare comunque necessaria un'opera di armonizzazione degli strumenti interni di cooperazione tra Stati dell'Unione Europea al fine di rendere più agevole il rapporto tra le diverse autorità investigative senza pregiudicare l'effettività delle garanzie difensive.

COMMENTO ALLE INFORMAZIONI PROVVISORIE DELLE SEZIONI UNITE IN RELAZIONE
ALL'UTILIZZABILITÀ DELLE CHAT CRIPTATE ACQUISITE IN FRANCIA TRAMITE O.E.I.

Note e riferimenti bibliografici

1. Secondo tale indirizzo giurisprudenziale, la messaggistica su "chat" di gruppo su sistema "Sky-ECC", acquisita mediante ordine europeo di indagine da autorità giudiziaria straniera che ne ha eseguito la decriptazione, costituisce 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. (Cass. Pen., Sez. 4, n. 16347 del 05/04/2023, Papalia, cit., secondo cui non rileva se i messaggi siano stati acquisiti dall'autorità giudiziaria straniera "ex post" o in tempo reale, poiché al momento della richiesta i flussi di comunicazione non erano in atto).
2. "in tema di misure cautelari personali, i gravi indizi di colpevolezza possono essere desunti da atti di indagine compiuti all'estero, in un diverso procedimento, da Autorità straniera, la cui utilizzabilità è subordinata all'accertamento, da parte del giudice italiano, non della loro regolarità ma del rispetto delle norme inderogabili e dei principi fondamentali dell'ordinamento, ferme restando la presunzione di legittimità dell'attività svolta e la competenza del giudice straniero in ordine alla verifica della correttezza della procedura e all'eventuale risoluzione di ogni questione relativa alle irregolarità riscontrate" (Sez. 1, n. 19082 del 13/01/2023 Cc., dep. 05/05/2023, rv. 284440, la quale, in applicazione del principio, ha ritenuto legittima l'utilizzazione di 'chat' intercorse sulla piattaforma di comunicazione criptata 'SKY ECC', acquisite mediante ordine europeo di indagine dall'autorità francese, che ne aveva eseguito la decriptazione).
3. Cfr. Cass. Pen., Sez. VI, n. 44154/23 (ric. Iaria Bruno): "Nel caso in esame non è chiaro quale parte delle iniziative istruttorie svolte all'estero risulti coperta da un non meglio delineato "segreto di Stato" apposto dall'autorità francese, di cui pure vi è menzione nel provvedimento impugnato, e in quale momento del procedimento di esecuzione dell'o.i.e. sia stato eventualmente opposto alle parti il segreto in questione."
4. cfr. pag. 10 Cass. Pen, Sez. I, n. 2312/24 (ric. Demce Elvis): "maggiormente condivisibile il consolidato orientamento giurisprudenziale sull'utilizzabilità degli atti trasmessi a seguito di attività di cooperazione internazionale (OEI e rogatoria), che non è condizionata a un accertamento da parte del giudice italiano sulla regolarità delle modalità di acquisizione esperite dall'autorità straniera, ritenendo valida - in assenza di deduzioni concrete e specifiche - la presunzione della regolarità dell'attività svolta, spettando al giudice straniero la verifica della correttezza della procedura e la competenza a risolvere qualsiasi questione in ordine alle eventuali irregolarità, da individuarsi specificamente" (in analoghi termini anche Cass. Pen. sez. V, sentenza n. 1405/2017; anche Cass. pen. sez. II, sentenza n. 24776/2010)".
5. 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, ric. Papalia
6. Cass. Pen., Sez. VI, n. 44154/23 (ric. Iaria) e Cass. Pen., Sez. VI, n. 44155/23 (ric. Kolgiokaj)
7. Sez. VI, n. 46482 del 27/9/2023, dep. 17/11/2023, ric. Bruzzaniti.
8. Sentenza Corte Costituzionale n. 170/23 resa nel giudizio per conflitto di attribuzioni tra il Senato e la Procura della Repubblica presso il Tribunale di Firenze in relazione all'acquisizione di plurime comunicazioni del senatore Matteo Renzi, disposta dalla Procura della Repubblica presso il Tribunale ordinario di Firenze nell'ambito del procedimento penale a carico dello stesso senatore e altri, in assenza di una previa autorizzazione da parte del Senato della Repubblica.
9. Ord. Rimessione Sez. Unite n. 47998/23 "a) Se in tema di mezzi di prova l'acquisizione di messaggi su chat di gruppo scambiati con sistema cifrato, mediante ^[Sky-ECC] presso A.G. straniera che ne ha eseguito la decriptazione, costituisca acquisizione di "documenti e di dati informatici" ai sensi dell'art. 234-bis cod. proc. pen. a mente del quale "è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare" o di documenti ex art. 234 cod. proc. pen. o sia riconducibile in altra disciplina relativa all'acquisizione di prove. b) Se inoltre, tale acquisizione debba essere oggetto, ai fini della utilizzabilità dei dati in tal modo versati in atti, di preventiva o successiva verifica giurisdizionale della sua legittimità da parte della Autorità giurisdizionale nazionale."

10. Ord. Rimessione Sez. Unite, Sez. VI, n. 2329/24: “1) Se l’acquisizione, mediante ordine europeo d’indagine, dei risultati dell’intercettazione disposti dall’Autorità giudiziaria estera su una piattaforma informatica criptata integri, o meno, l’ipotesi disciplinata dall’ordinamento interno all’art. 270 c.p.p. 2) Se l’acquisizione, mediante l’ordine europeo d’indagine, dei risultati dell’intercettazione disposti dall’Autorità giudiziaria estera attraverso l’inserimento di un captatore informatico sul server di una piattaforma criptata sia soggetta nell’ordinamento interno ad un controllo giurisdizionale, preventivo o successivo, in ordine all’utilizzabilità dei dati raccolti”

11. cfr. Cass. Pen., Sez. I, n. 13535/24 dep. 3 aprile 2024

12. Cfr. pag. 27 della Memoria della Procura Generale depositata dinanzi alle Sezioni Unite della Suprema Corte per l’udienza del 29 febbraio 2024: “Trattasi di provvedimento emesso dall’autorità giudiziaria francese, con ampia e specifica motivazione e secondo standard addirittura superiori a quelli previsti nell’ordinamento nazionale italiano: infatti, nella motivazione – ben oltre i requisiti minimi di cui all’art. 267 c.p.p. – è argomentata l’indispensabilità del mezzo (cfr. ALL. n. 5)11. A questo provvedimento, nel febbraio 2021, ha fatto seguito un altro provvedimento, sempre del giudice istruttore di Parigi, per l’installazione di un secondo “dispositif de captation de données” (cfr. ALL. n. 6). A questo punto, acquisite grazie alle intercettazioni le chiavi di cifratura che erano conservate nei server e recuperati a mezzo di trojan gli algoritmi di decodifica che erano riposti nei criptofonini, la polizia giudiziaria francese ha potuto decodificare i messaggi già registrati e apprendere il significato di quelli che intervenivano successivamente (cfr. atti in ALL. 1). In seguito, il 9 marzo 2021, la polizia giudiziaria ha eseguito una operazione su base internazionale, così rendendo pubblica l’avvenuta violazione del sistema criptato, con l’accesso ai “flussi di informazione di oltre 70.000 utenti”.

13. ex multis Cass. Pen., Sez. III, n. 24305/17, Cass. Pen., Sez. VI, n. 12722/09 - dep. 23/03/2009, P.M. in proc. Lombardi Stronati e altri, Rv. 243241

14. "La libertà e la segretezza delle comunicazioni nell’ordinamento costituzionale” di Corrado Caruso

15. Cfr. art. 100 – 1 e 2 Code de procédure pénal (Modifié par LOI n°2021-1729 du 22 décembre 2021 - art. 3): “En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à trois ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques. Ces opérations sont effectuées sous son autorité et son contrôle. **La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.**”

16. cfr. Cass. Pen., Sez. III, n. 15828/15

17. Il diritto alla riservatezza della corrispondenza e di ogni mezzo di comunicazione non è che un aspetto essenziale della stessa inviolabilità della persona, e perciò è direttamente riconducibile nella categoria dei diritti inviolabili dell'uomo. Pertanto, una deroga al libero esercizio di quel diritto non solo dev'essere giustificata da preminenti ragioni di pubblico interesse, ma non può attuarsi se non con le garanzie che consentano un'efficace verifica della sua legittimità. E non a caso, infatti, ancor prima dell'entrata in vigore del nuovo codice, è stato proprio in tale specifica materia che si venuta a delineare, ed in maniera prioritaria ed improcrastinabile, la necessità di affidare alla sanzione della inutilizzabilità il compito di garantire il procedimento acquisitivo della prova, allorché questo poteva arrecare offesa a quel diritto di libertà che è così indissociabile dal doveroso rispetto della persona.” (cfr. Sez. Unite n. 5021/1996)

18. ex multis Sez. VI, n. 9009 del 4/04/2020, Rv. 278563; Sez. V, n. 44114/19 del 10/10/19, Rv. 277432

19. Cfr. pag. 63 Memoria del P.G. depositata dinanzi alle Sezioni Unite della Suprema Corte per l’udienza del 29 febbraio 2024 : “Bisognerebbe ritenere, altrimenti, che il diritto alla riservatezza delle conversazioni criptate – una sorta di diritto “tiranno” - sia onnivoro e prevalga sempre e comunque rispetto alla azione dello Stato (recte: degli Stati) per l’accertamento dei reati, senza alcuna possibilità di bilanciamento, anche in un caso in cui, in forza di specifici OEI, siano state acquisite soltanto determinate conversazioni relative a specifici soggetti, i quali, in sostanza, da indagati per un massivo narcotraffico intercontinentale di stupefacenti, si trasformano in paladini della minacciata legalità per i terzi estranei, co-fruitori della medesima piattaforma criptata, dolendosi della lesione della riservatezza di detti terzi, non indagati, anzi, persino non identificati, e le cui conversazioni non sono emerse nel corso delle indagini, né prese in considerazione in esse, né lo saranno mai.”

20. Cfr. pagg. 83-84 Memoria del P.G. depositata dinanzi alle Sezioni Unite della Suprema Corte per l’udienza del 29 febbraio 2024 “il Conseil constitutionnel francese, con la decisione n. 2022-987 QPC dell’8 aprile 2022, ha

statuito che la disciplina francese, sulla cui base è stata disposta l'acquisizione delle chat e l'intercettazione delle comunicazioni operate nel presente procedimento, è conforme alla Costituzione francese; il Bundesgerichtshof, 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".

21. "Ordine europeo di indagine penale e comunicazioni criptate: il caso skyEcc/Encrochat in attesa delle Sezioni Unite" di Marcello Daniele

22. Domanda di pronuncia pregiudiziale proposta dal Landgericht Berlin (Germania) il 24 ottobre 2022 — procedimento penale a carico di M.N. (Causa C-670/22 - 2023/C 35/37) (cfr. Gazzetta ufficiale dell'Unione europea - C 35/31 - 30/01/23)

23. Avvocato generale Ćapeta: un pubblico ministero può emettere un ordine europeo di indagine (OEI) diretto al trasferimento di prove già raccolte in un altro Stato membro (Comunicato Stampa 163/23, Lussemburgo 26 ottobre 2023, Conclusioni dell'avvocato generale nella causa C-670/22, Staatsanwaltschaft Berlin (EncroChat))

24. Corte Giust., 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e 520/18

25. "In particolare, dall'informativa sull'andamento delle indagini del "Brigadiere di polizia" al pubblico ministero del 18 luglio 2019, emerge che "un'analisi preliminare del flusso di rete ha rivelato elementi promettenti: parte del traffico di rete non è stato crittografato; alcune informazioni sono passate in chiaro; un'analisi sintetica dei primi pacchetti di rete intercettati ha consentito di risalire ai clienti delle email di conferma dell'attivazione dell'account SKY ECC compreso il numero IMEI, il numero" seriale del telefono attivato, l'identificativo SK YECC, ecc.). (cfr. pag. 26 memoria del P.G. in vista delle Sezioni Unite del 29 febbraio 2024)

26. cfr. Nota del Brigadier de Police Guillaume Lamboy del 19 giugno 2019: "L'enquête débutait en Belgique suite à une affaire de trafic de produits stupéfiants dans le port d'Anvers avec la saisie de téléphones chiffrés dont l'application SKYECC était installée pour communiquer discrètement. Il était ensuite établi par les autorités précitées que l'utilisation de la solution SKYECC servait exclusivement pour faciliter des activités criminelles. Il était mentionné notamment des dizaines de dossiers de la Police Judiciaire d'Anvers relatifs à des organisations criminelles utilisant des appareils SKYECC. Plus de 350 numéros SKYECC étaient impliqués juste pour la zone d'Anvers. Ce chiffre montait à 1000 numéros reliés à des activités criminelles sur l'ensemble du territoire belge. Les autorités belges précisaient également que la société SKYECC ne collaborait pas avec les forces de l'ordre, même après l'obtention d'un mandat du juge. Les autorités belges et néerlandaises indiquaient qu'il y avait environ 68 000 utilisateurs de l'application dans le monde dont la majorité en Europe, environ 8000 utilisateurs en Belgique et plus de 100 000 sessions de données par jour."

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:

<https://rivista.camminodiritto.it/articolo.asp?id=10436>