



COMMENTO ALLE SENTENZE DELLE SEZIONI UNITE RELATIVE AL CASO DEI C.D. "CRIPTOFONINI"

Le Sezioni Unite hanno depositato le motivazioni delle sentenze relative al caso dei c.d. criptofonini. Con tali pronunce, le Sezioni Unite hanno concluso allo stato per la legittimità dell'acquisizione delle chat da parte dei PM italiani attraverso lo strumento di cooperazione giudiziaria dell'Ordine europeo di indagine (O.E.I.). Pertanto, tali acquisizione probatorie potranno essere utilizzate legittimamente nel quadro di procedimenti penali interni in applicazione della disciplina prevista dal combinato disposto degli artt. 78 disp. att. c.p.p., 238 e 270 c.p.p.

di Vincenzo Scarlato
IUS/16 - DIRITTO PROCESSUALE PENALE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Alessio Giaquinto

Publicato, Martedì 25 Giugno 2024

Sommario: 1. Premessa storica. L'indagine condotta dalle Autorità investigative straniere; 2. 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.; 3. La discontinuità determinata dalle sentenze di annullamento con rinvio della Sesta Sezione Penale e i dubbi interpretativi sulla disciplina normativa applicabile; 4. L'inquadramento delle chat criptate quale sequestro di corrispondenza telematica all'esito della sentenza n. 170/23 della Corte Costituzionale; 5. Gli orientamenti contrapposti e le ordinanze di rimessione alle Sezioni Unite della Suprema Corte di Cassazione; 6. La necessità di acquisizione dei provvedimenti autorizzativi e dei verbali delle operazioni relativi agli esiti delle intercettazioni acquisiti ex artt. 78 disp. att. c.p.p., 238 e 270 c.p.p. dal procedimento francese; 7. Riflessioni critiche relative alle pronunce delle Sezioni Unite; 8. Conclusioni.

1. Premessa storica

In data 14 giugno 2024 sono state depositate le motivazioni delle pronunce gemelle di cui alle informazioni provvisorie n. 3 e 4 del 2024 (cfr. Cass. Pen., Sez. Unite, Pres. Cassano, Est. Corbo, n. 23755 e 23756, ud. 29 febbraio 2024, dep. 14 giugno 2024)^[1]. Va premesso che le pronunce in questione avevano ad oggetto il caso relativo ai criptofonini. In data 29 febbraio 2024 erano già state depositate le informazioni provvisorie^[2] relative alle suddette pronunce. Da tali informazioni provvisorie si poteva evincere che le Sezioni Unite avevano sostanzialmente legittimato l'utilizzazione nei procedimenti penali interni degli elementi acquisiti attraverso l'attività di intercettazione dei c.d. "criptofonini" sviluppatasi nel quadro di un procedimento penale francese. L'attività captativa in questione aveva consentito lo smantellamento della piattaforma di comunicazione criptata denominata "skyEcc" con la conseguente captazione e decriptazione di tutte le conversazioni riconducibili agli utenti della suddetta piattaforma criptata. Tale attività captativa aveva coinvolto circa 100.000 utenti localizzati in diversi Stati del mondo, soprattutto in Europa. In Italia è stato calcolato un numero approssimativo di circa 15.000 utilizzatori del sistema di comunicazione criptata skyEcc. 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.

Le Sezioni Unite, dopo aver ripercorso i vari orientamenti giurisprudenziali contrapposti, hanno concluso comunque per la legittimità dell'utilizzazione nei procedimenti penali interni degli elementi indiziari acquisiti all'esito della suddetta attività investigativa in applicazione delle disposizioni di cui agli artt. 78 disp att. C.p.p., 238 c.p.p. e 270 c.p.p.^[3]

Nella pronuncia gemella n. 23756/24 (ric. Giorgi), le Sezioni Unite confermavano la suddetta interpretazione precisando che, in materia di ordine europeo d'indagine, l'acquisizione degli esiti di intercettazioni effettuate nel quadro di un procedimento estero andasse ricondotta alla disciplina di cui all'art. 270 c.p.p.^[4] Di conseguenza, entrambe le pronunce hanno aderito ad un orientamento che ritiene pacificamente utilizzabili, nei procedimenti penali interni, gli elementi di prova acquisiti nel procedimento penale francese mediante le intercettazioni dei flussi di comunicazioni transitanti sui server e dei dati informatici custoditi all'interno dei server in uso alla piattaforma criptata skyECC localizzati in Francia a Roubaix.

2. 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.

Bisogna premettere che la giurisprudenza nazionale aveva immediatamente aderito all'impostazione secondo cui l'acquisizione delle prove rappresentate dagli estratti delle comunicazioni criptate skyEcc già in possesso dell'A.G. francese andava sempre considerata legittima, trattandosi di acquisizione di dati informatici già detenuti legittimamente dal legittimo titolare ovvero lo Stato francese^[5].

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^[6].

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. Si censurava altresì l'assenza totale di motivazione specifica in merito al collegamento tra l'indagine in corso e le singole utenze abbinate 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. avente ad oggetto gli esiti di operazioni di intercettazioni di comunicazioni con conseguente inutilizzabilità delle prove acquisite attraverso il suddetto strumento in assenza di un vaglio giurisdizionale interno.

In sintesi, ad avviso delle difese, allorché 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^[7]

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^[8].

Ne consegue come 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 poneva l'interprete era 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 delle modalità 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.^[9].

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 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.

3. 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^[10]. 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.

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

Una successiva sentenza^[11] 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^[12] relativa ad un'ipotesi di sequestro probatorio di corrispondenza riconducibile ad un parlamentare, aveva 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.

5. Gli orientamenti contrapposti e le ordinanze di rimessione alle Sezioni Unite della Suprema Corte di Cassazione

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^[13] del 30 novembre 2023 e la Sesta Sezione Penale con l'ordinanza n. 2329^[14] 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.).

6. 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 un'ultima pronuncia della Suprema Corte^[15] 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 e i verbali relativi all'esecuzione delle operazioni di intercettazioni dei flussi di comunicazioni.

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.

7. Riflessioni critiche relative alle pronunce delle Sezioni Unite

Alla luce delle informazioni provvisorie depositate in data 29 febbraio 2024, possiamo concludere che le motivazioni delle Sezioni Unite si rivelano coerenti con le informazioni provvisorie a suo tempo depositate. Tuttavia, le conclusioni delle Sezioni Unite, pur condivisibili in ordine alla riconduzione della circolazione transfrontaliera di prove alle disposizioni di cui agli artt. 78 disp att. C.p.p., 238 c.p.p. e 270 c.p.p., non possono assolutamente essere condivise in relazione alla legittimità dell'attività investigativa così come sviluppatasi ab origine nel quadro del procedimento a quo francese.

In particolare, non può essere condivisa la conclusione secondo la quale è consentito ad uno Stato straniero eseguire intercettazioni in Italia senza comunicarlo allo Stato italiano^[16]. Nel caso di specie, è emerso che, nel corso delle investigazioni portate avanti dalle Autorità investigative francesi, queste ultime avevano avuto modo di apprendere che gli utilizzatori dei criptofonini erano localizzati in diversi Stati d'Europa^[17].

Tuttavia, lo Stato francese non ha richiesto alcun tipo di assistenza giudiziaria ai diversi Stati in cui erano ubicati i diversi soggetti coinvolti dall'attività captativa in questione né ha notificato loro l'esecuzione delle suddette operazioni.

Ciò ha determinato una palese violazione del diritto dell'Unione Europea. Ciò va sottolineato a prescindere dal fatto che i PM italiani abbiano acquisito nei procedimenti interni elementi di prova già cristallizzati nel quadro di un procedimento penale sviluppatosi all'estero. A tal proposito va ribadito come la presunzione di legittimità dell'attività investigativa svolta all'estero sia soltanto relativa.

Da ciò discende che tale presunzione possa essere superata da specifiche deduzioni attinenti il mancato rispetto dei diritti fondamentali. Pertanto, risulta influente che l'acquisizione "a valle" avesse ad oggetto un elemento di prova già acquisito laddove la suddetta acquisizione risultasse "a monte" viziata dal mancato rispetto delle garanzie

procedurali previste ad hoc della normativa sovranazionale.

Infatti, l'art. 31 comma 2 Direttiva n. 41/14^[18] prevede che venga trasmessa la notifica attraverso il modello C allo Stato membro in cui si intende eseguire l'intercettazione nel caso di intercettazioni senza necessità di assistenza dello Stato straniero.

Diversamente, è previsto che la notifica avvenga durante le operazioni d'intercettazione nel caso in cui lo Stato non sappia che le attività d'intercettazione si svilupperanno nei confini dello Stato estero. In tal caso, laddove dovesse emergere la consapevolezza di svolgere operazioni d'intercettazione nel territorio di un altro Stato, sarà necessario notificarlo immediatamente all'A.G. del suddetto Stato.

Ciò al fine di consentire allo Stato, i cui cittadini siano stati oggetto d'intercettazione da parte di uno Stato straniero, di inibire la prosecuzione delle operazioni nei casi in cui non siano ammesse in un caso interno analogo ovvero di circoscriverne preventivamente le condizioni di utilizzabilità.

Anche l'art. 24 del d.lgs. n. 108/17^[19] prescrive al Procuratore della Repubblica di informare immediatamente il Giudice per le indagini preliminari non appena abbia notizia che sono in corso operazioni d'intercettazione nel territorio dello Stato.

Peraltro, la Corte di Giustizia dell'Unione Europea a seguito di rinvio pregiudiziale promosso dal Tribunale di Berlino (C-670/22) in relazione al caso “Encrochat” ha evidenziato che l'art. 31 Direttiva n. 41/14 deve essere interpretato nel senso che “esso mira anche a tutelare i diritti degli utenti interessati da una misura di «intercettazione di telecomunicazioni», ai sensi di tale articolo”.

Nel caso di specie, non risulta alcuna notifica effettuata allo Stato italiano con le formalità prescritte dalla normativa sovranazionale e dalla normativa interna di recepimento. Ma soprattutto risulta in modo evidente il coinvolgimento (quantomeno dal gennaio 2021) delle Autorità investigative italiane^[20] che, non appena notiziate dalle Autorità francesi in merito alle operazioni captative in corso in territorio italiano, avrebbero dovuto trasmettere immediatamente al Giudice per le indagini preliminari la notificazione di avvio delle operazioni effettuate dalla Francia. Va aggiunto che l'art. 44 D.lgs. n. 108/17^[21] è rubricato come “Obblighi di informazione in favore dell'autorità giudiziaria di altro Stato membro”. La norma appena richiamata detta in modo espresso le condizioni per attivare un'intercettazione in uno Stato estero. Pertanto, lo Stato italiano, nel caso in cui voglia procedere ad operazione di intercettazione in uno Stato estero sarà obbligato a rispettare quanto prescritto dall'art. 44, comma 1 D.lgs. n. 108/17 ovvero informare mediante il modello C l'Autorità giudiziaria dello Stato estero.

Ne consegue come risulti in modo lampante il mancato rispetto da parte della Francia delle suddette garanzie procedurali. Infatti, in assenza della procedura prescritta, in un caso analogo lo Stato italiano non avrebbe potuto procedere ad intercettazioni all'estero. E' evidente che le garanzie previste dalla legge (costituzionale e sovranazionale) non sono state rispettate per l'esecuzione di operazioni d'intercettazione da parte di uno Stato straniero nei nostri confini nazionali. L'art. 15 comma 2 Cost. prevede che la limitazione dell'inviolabilità delle comunicazioni possa avvenire solo dietro atto motivato dell'Autorità giudiziaria e con le garanzie stabilite dalla legge^[22].

Ad avviso dello scrivente, un'attività di intercettazione di un soggetto residente in uno Stato straniero posta in essere senza il rispetto delle suddette garanzie andrà considerata inevitabilmente in contrasto con i principi fondamentali trasfusi nella nostra Costituzione. Ciò dovrà determinare l'inutilizzabilità del materiale indiziario acquisito senza il rispetto delle suddette garanzie procedurali.

Peraltro, l'assenza di sanzioni previste in caso di mancato rispetto della procedura di cui all'art. 31 Dir. 41/14 non può essere condivisa perché lascerebbe una totale discrezionalità agli Stati in ordine alla necessità di provvedere alla notifica allo Stato straniero attinto dall'esecuzione delle operazioni captative.

In sostanza, gli Stati stranieri potranno procedere autonomamente senza alcuna conseguenza ad operazioni di intercettazione di massa all'interno dei confini nazionali di altri Stati. Che senso ha prevedere delle specifiche procedure ad hoc e non prevedere sanzioni nel caso in cui non vengano rispettate? Purtroppo, l'interrogativo non trova alcuna risposta al momento. Peraltro, appare evidente che l'unica conseguenza di un'operazione di intrusione indebita nelle comunicazioni dei cittadini da parte di uno Stato straniero sarà l'eventuale inutilizzabilità del materiale indiziario acquisito ma, esclusivamente in caso di violazione dell'art. 270 c.p.p.

Peraltro, seguendo le indicazioni ricavabili dall'informazione provvisoria n. 7/2024^[23] in relazione alla portata applicativa dell'art. 270 c.p.p., per i soli procedimenti iscritti tra il 31 agosto 2020 e il 10 agosto 2023, bisognerà applicare l'art. 270 c.p.p. nella sua versione antecedente rispetto al D.L. n. 105/23. Infatti, l'art. 270 c.p.p., nella sua versione antecedente al 10 agosto 2023, prevedeva la possibilità di utilizzazione dei risultati di intercettazioni in procedimenti diversi da quello in cui venivano autorizzate per tutti i reati per i quali era consentito il ricorso alle intercettazioni di cui all'art. 266 c.p.p. (ovvero i reati puniti con una pena edittale massima non inferiore a 5 anni). Le Sezioni Unite hanno circoscritto il perimetro di applicabilità dell'art. 270 c.p.p. nella sua versione precedente ai soli procedimenti iscritti dopo il 31 agosto 2020.

Tuttavia, nel caso di specie, il procedimento originario francese risale al 2019^[24]. Di conseguenza, nei procedimenti interni non sarà applicabile la disposizione di cui all'art. 270 c.p.p. che estendeva la possibilità di utilizzazione degli esiti delle intercettazioni in procedimenti diversi per tutte le ipotesi previste dal catalogo di cui all'art. 266 c.p.p.

8. Conclusioni

In definitiva, gli elementi di prova acquisiti attraverso le operazioni d'intercettazione eseguite nel procedimento penale francese saranno utilizzabili in tutti i procedimenti penali interni a condizione che i procedimenti penali interni abbiano ad oggetto l'accertamento di ipotesi di reato per le quali è previsto l'arresto obbligatorio in flagranza ex art. 380 c.p.p.

Ad avviso dello scrivente, l'interpretazione fornita dalle Sezioni Unite può rappresentare un pericolo per la nostra democrazia. Infatti, con l'avallo di queste forme di intrusione occulte di Stati stranieri, tutti i cittadini italiani potrebbero facilmente essere intercettati e ricattati dagli Stati stranieri (rectius: da gruppi di Stati stranieri). Peraltro, potendo intercettare impunemente un vasto numero di soggetti, gli Stati stranieri potrebbero utilizzare legittimamente lo strumento captativo per scopi illeciti ovvero per reperire informazioni relative alla nostra sicurezza nazionale.

La possibilità di successiva utilizzazione processuale del materiale acquisito contro i cittadini italiani attraverso tali modalità potrebbe condizionare la libertà dei cittadini e, in alcuni casi, di cittadini con posizioni apicali all'interno dello Stato. Tuttavia, al fine di salvaguardare l'utilizzo delle prove acquisite dalla Francia con queste modalità opache, le Sezioni Unite hanno abbracciato un orientamento che legittima gli Stati esteri a monitorare impunemente tutti i nostri cittadini senza alcun vaglio preventivo giurisdizionale di un giudice nazionale italiano e senza alcuna sanzione d'inutilizzabilità in caso di mancato rispetto delle procedure dettate ad hoc dalla normativa sovranazionale ed interna di recepimento.

Appare inaccettabile legittimare il mancato rispetto della procedura di notifica allo Stato estero prevista dall'art. 31 Dir. 41/14 con l'esclusione di sanzioni in caso di inosservanza della suddetta procedura. Ciò degraderebbe l'informazione allo Stato estero ad un mero adempimento formale laddove la notifica allo Stato estero dovrebbe consentire il rispetto delle garanzie di sovranità territoriale del suddetto Stato e di tutela delle comunicazioni dei propri cittadini.

Se è questo lo stato dell'arte bisogna concludere che la garanzia di tutela costituzionale

dei valori fondamentali dei cittadini è stata ritenuta recessiva rispetto al securitarismo giustizialista di stampo transnazionale. In ogni caso, l'auspicio dello scrivente è che un intervento della Corte Costituzionale possa ripristinare le garanzie previste dall'art. 15 della Costituzione dichiarando l'illegittimità costituzionale della normativa interna di recepimento della Direttiva n. 41/14 trasfusa nel D.lgs. n. 108/17 nella parte in cui non prevede l'inutilizzabilità delle intercettazioni eseguite dagli Stati stranieri in violazione delle disposizioni previste dalla Direttiva n. 41/14 e, in particolare, dell'art. 31 della suddetta direttiva.

L'intervento della Corte Costituzionale risulta fondamentale anche alla luce della pronuncia della Corte di Giustizia dell'Unione Europea resa nell'ambito del giudizio su rinvio pregiudiziale del Tribunale del Land di Berlino nel caso "Encrochat" (Causa n. 670/22 del 30 aprile 2024)^[25]. Infatti, la CGUE ha affermato che, allo stato attuale del diritto dell'Unione, spetta, in linea di principio, unicamente al diritto nazionale determinare le norme relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale, di elementi di prova che sono stati ottenuti con modalità contrarie al diritto dell'Unione.

Pertanto, la CGUE ha lasciato una sostanziale discrezionalità agli Stati membri in ordine al rispetto del diritto dell'Unione con la conseguenza che eventuali inosservanze del diritto dell'unione europea nel procedimento di acquisizione probatoria potrebbero restare sfornite di sanzioni nei procedimenti penali interni^[26]. In conclusione, con l'auspicio di un tempestivo intervento della Corte Costituzionale italiana in ordine ai profili di illegittimità costituzionale evidenziati, appare assolutamente 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.

Note e riferimenti bibliografici

[1] Cfr. Cass. Pen., Sez. Unite, n. 23755/24 e 23756/24

[2] Cfr. Informazione provvisoria delle Sezioni Unite n. 3 e 4 del 29 febbraio 2024

[3] Cfr. Cass. Pen., Sez. Unite n. 23755/24, Pres. Cassano, Rel. Corbo, Ric. Gyuzi Ermal - pag. 38 “In considerazione delle argomentazioni si qui esposte vanno enunciati i seguenti principi di diritto: La trasmissione, richiesta con ordine europeo d’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 c.p.p. e 78 disp. Att. Cod. proc. pen.”

[4] Cfr. Cass. Pen., Sez. Unite, n. 23756/24, Pres. Cassano, rel. Corbo, Ric. Giorgi – pag. 47 “In considerazione delle argomentazioni fin qui esposte, vanno affermati i seguenti principi di diritto: In materia di ordine europeo d’ 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.”

[5] 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).

[6] “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 straniere, 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).

[7] 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.”

[8] 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)”.

[9] 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

[10] Cass. Pen., Sez. VI, n. 44154/23 (ric. Iaria) e Cass. Pen., Sez. VI, n. 44155/23 (ric. Kolgiokaj)

[11] Sez. VI, n. 46482 del 27/9/2023, dep. 17/11/2023, ric. Bruzzaniti.

[12] 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.

[13] 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 decrittazione, 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.”

[14] 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”

[15] cfr. Cass. Pen., Sez. I, n. 13535/24 dep. 3 aprile 2024

[16] Cfr. pp. 46-47 Cass. Pen., Sez. Unite n. 23756/24: “Con riferimento alle garanzie previste dalla Direttiva 2014/41/UE, può venire in rilievo il profilo, segnalato dai ricorrenti, della violazione dei principi fissati dall'art. 31 in ordine alle intercettazioni effettuate nei confronti di persone il cui «indirizzo di comunicazione» è utilizzato nel territorio di uno Stato diverso da quello nel quale le operazioni di captazione sono state disposte. Secondo quanto più analiticamente esposto in precedenza al § 15.2, l'art. 31 Direttiva cit. prevede che lo Stato nel quale sono state disposte le intercettazioni dia «notifica» di tali attività all'autorità competente nello Stato nel quale è utilizzato l'indirizzo di comunicazione sottoposto a controllo, quando viene a conoscenza di tale circostanza, e che quest'ultima possa vietare il compimento o la prosecuzione delle operazioni, nonché l'utilizzazione dei risultati già ottenuti. Sulla base di tale disciplina, deve rilevarsi, innanzitutto, che l'obbligo di notifica sorge quando l'autorità precedente viene a conoscenza che l'intercettazione riguarda persone il cui «indirizzo di comunicazione» è utilizzato nel territorio di un altro Stato. Va segnalato, poi, che l'eventuale intempestività della comunicazione non è sanzionata di per sé, e che, in ogni caso, opera la garanzia della possibile dichiarazione di inutilizzabilità da parte dell'autorità competente dello Stato in cui è fatto uso dell'«indirizzo di comunicazione». Occorre considerare, ancora, che il divieto della Direttiva 2014/41/UE di iniziare o proseguire le attività di captazione, ovvero di utilizzarne i risultati, è previsto solo «^qualora 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.”

[17] 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.”

[18] Articolo 31 Dir. 41/14 **Notifica allo Stato membro nel quale si trova la persona soggetta a intercettazione e la cui assistenza tecnica non è necessaria**: “1. Se, ai fini del compimento di un atto di indagine, l'intercettazione di telecomunicazioni è autorizzata dall'autorità competente di uno Stato membro (lo «Stato membro di intercettazione») e l'indirizzo di comunicazione della persona soggetta a intercettazione indicata nell'ordine di intercettazione è utilizzato sul territorio di un altro Stato membro (lo «Stato membro notificato») la cui assistenza tecnica non è necessaria per effettuare l'intercettazione, lo Stato membro di intercettazione ne dà notifica all'autorità competente dello Stato membro notificato dell'intercettazione: a) prima dell'intercettazione, qualora l'autorità competente dello Stato membro di intercettazione sappia, al momento di ordinare l'intercettazione, che la persona soggetta a intercettazione e si trova o si troverà sul territorio dello Stato membro notificato; b) durante l'intercettazione o ad intercettazione effettuata, non appena venga a conoscenza del fatto che la persona soggetta a intercettazione si trova, o si trovava durante l'intercettazione, sul territorio dello Stato membro notificato. 2. La notifica di cui al paragrafo 1 è effettuata utilizzando il modulo di cui all'allegato C. 3. Qualora l'intercettazione non sia ammessa in un caso interno analogo, l'autorità competente dello Stato membro notificato può, senza ritardo e al più tardi entro 96 ore dalla ricezione della notifica di cui al paragrafo 1, notificare all'autorità competente dello Stato membro di intercettazione che: a) l'intercettazione non può essere effettuata o si pone fine alla medesima; e b) se necessario, gli eventuali risultati dell'intercettazione già ottenuti mentre la persona soggetta ad intercettazione si trovava sul suo territorio non possono essere utilizzati o possono essere utilizzati solo alle condizioni da essa specificate. L'autorità competente dello Stato membro notificato informa l'autorità competente dello Stato membro di intercettazione dei motivi di tali condizioni. 4. L'articolo 5, paragrafo 2, si applica, mutatis mutandis, alla notifica di cui al paragrafo 2.”

[19] Art. 24 Notifica all'autorità giudiziaria italiana nel caso di persona soggetta a intercettazione nel territorio dello Stato 1. Quando è disposta, senza richiesta di assistenza tecnica, l'intercettazione di un dispositivo, anche di sistema informatico o telematico, in uso a persona che si trovi nel territorio dello Stato, il procuratore della Repubblica, trasmette immediatamente al giudice per le indagini preliminari la notificazione dell'avvio delle operazioni effettuata dall'autorità giudiziaria dello Stato membro che procede. 2. Il giudice per le indagini preliminari ordina l'immediata cessazione delle operazioni se le intercettazioni sono state disposte in riferimento a un reato per il quale, secondo l'ordinamento interno, le intercettazioni non sono consentite e ne dà contestuale comunicazione al procuratore della Repubblica. 3. Il procuratore della Repubblica senza ritardo, e comunque non oltre novantasei ore dalla ricezione della notifica, dà comunicazione all'autorità giudiziaria dello Stato membro del provvedimento di cessazione delle operazioni e della non utilizzabilità a fini di prova dei risultati delle intercettazioni eseguite.

[20] Cfr. pag. 13 informativa ROS Reggio Calabria processo “Eureka” “Tali argomentazioni, quindi inducevano questo Reparto ad avviare, fin dal gennaio 2021, di intesa con codesta A.G., intensi rapporti di cooperazione, sul fronte di polizia, con l'agenzia europea Europol presso cui erano state create specifiche task force operative a seguito della violazione dei server di ENCROCHAT e SKYECC e riversati tutti i dati intercettati.” Cfr. pag. 13 informativa ROS Reggio Calabria”

[21] Art. 44 Obblighi di informazione in favore dell'autorità giudiziaria di altro Stato membro 1. Il pubblico ministero, prima di dare inizio alle operazioni di intercettazione, informa, mediante trasmissione del modello di cui all'allegato C al presente decreto, l'autorità giudiziaria competente dello Stato membro nel cui territorio si trova il

dispositivo o il sistema da controllare. 2. Nel corso delle operazioni di intercettazione, il pubblico ministero, non appena ha notizia che il dispositivo o il sistema controllato si trova nel territorio di altro Stato membro, provvede immediatamente, con le modalità di cui al comma 1, a dare informazione all'autorità giudiziaria competente dello Stato membro interessato che le operazioni di intercettazione sono state avviate e sono in corso. 3. Il pubblico ministero dispone l'immediata cessazione delle operazioni di intercettazione quando l'autorità giudiziaria dello Stato membro, ricevuta l'informazione di cui ai commi 1 e 2, comunica che non possono essere eseguite o proseguite. I risultati dell'intercettazione possono comunque essere utilizzati alle condizioni stabilite dall'autorità giudiziaria dello Stato membro.

[22] Art. 15 Cost.: “La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.

La loro limitazione può avvenire solo per atto motivato dell'autorità giudiziaria e con le garanzie stabilite dalla legge”

[23] Cfr. Informazione provvisoria delle Sezioni Unite n. 7/2024

[24] Cfr. provvedimento di intercettazione del Juge des libertés et de la détention Ali Haroune: “Le 13 février 2019, le procureur de la République près le T.G.I. de Lille décidait d'ouvrir une enquête préliminaire concernant la société SKYECC”

[25] Sentenza della CGUE nella causa C-670/22 | M.N. (EncroChat)

[26] Cfr. punto 128-129 della sentenza della CGUE nella causa n. 670/22 (caso “Encrochat”): “Dall’altro, allo stato attuale del diritto dell’Unione, spetta, in linea di principio, unicamente al diritto nazionale determinare le norme relative all’ammissibilità e alla valutazione, nell’ambito di un procedimento penale, di informazioni e di elementi di prova che sono stati ottenuti con modalità contrarie al diritto dell’Unione (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 222). Infatti, secondo una costante giurisprudenza, in assenza di una normativa dell’Unione in materia, spetta all’ordinamento giuridico interno di ciascuno Stato membro, ai sensi del principio dell’autonomia procedurale, stabilire le modalità procedurali dei ricorsi intesi a garantire la tutela dei diritti spettanti ai singoli in forza del diritto dell’Unione, a condizione tuttavia che esse non siano meno favorevoli rispetto a quelle relative a situazioni analoghe assoggettate al diritto interno (principio di equivalenza) e che non rendano in pratica impossibile o eccessivamente difficile l’esercizio dei diritti conferiti dal diritto dell’Unione (principio di effettività) (v., in tal senso, sentenze del 16 dicembre 1976, Rewe-Zentralfinanz e Rewe-Zentral, 33/76, EU:C:1976:188, punto 5, e del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 223).”

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

<https://rivista.camminodiritto.it/articolo.asp?id=10592>