

L'utilizzabilità delle chat criptate SkyEcc al vaglio delle Sezioni Unite: analisi del dibattito e prospettive di riforma del codice di rito

di Giuseppe Amato, giudice presso il Tribunale del Riesame di Reggio Calabria

1. Introduzione – 2. Il contrasto sorto nella giurisprudenza della Corte di Cassazione - 3. Gli elementi “esterni” rilevanti: la giurisprudenza della Corte Costituzionale e quella della Corte di Giustizia dell’Unione Europea – 4. Conclusioni e prospettive *de iure condendo*

1. Introduzione

Il progresso delle tecnologie informatiche e con esse delle modalità di comunicazione tra consociati per via telematica è fenomeno che ha apportato indubbi vantaggi nella conduzione della vita quotidiana di ognuno di noi, permettendo sempre maggiore rapidità di connessione e semplicità nell’interagire in forma orale e scritta.

Tuttavia, non può non rilevarsi come tale processo di continua evoluzione trovi l’altro lato della medaglia nell’impiego di tali strumenti tecnologicamente avanzati da parte di soggetti impegnati nella conduzione di traffici illeciti e, per quanto finora appurato dalle indagini condotte da diverse Procure di Stati comunitari (in particolare, Italia, Francia, Belgio e Olanda), particolarmente nel settore del narcotraffico internazionale.

I più recenti risvolti investigativi hanno infatti avuto modo di appurare come, per il tramite dell’utilizzo di applicazioni di chat criptate denominate SkyEcc e Encrochat, vari soggetti impegnati nel settore del narcotraffico riuscissero, in maniera di fatto indisturbata, a organizzare l’importazione, la detenzione e la successiva commercializzazione di ingentissime quantità di cocaina provenienti dal Sud America e approdate nei porti europei di Gioia Tauro, Anversa e Rotterdam.

Tali traffici sono stati scoperti a seguito dell’attività svolta da squadre comuni di investigazione (Joint Investigation Team) tra le autorità inquirenti della Francia, del Belgio e dell’Olanda.

A seguito di attività di captazione di flussi di dati tra i server di proprietà della società informatica OVH, siti nella città di Roubaix (sui quali poggiava l’intera struttura telematica della Sky Global, società creatrice e gestore dell’applicazione di messaggistica criptata denominata SkyEcc), è stato possibile acquisire sia il flusso di comunicazioni consistenti nel contenuto dei messaggi scambiati dagli utenti delle succitate applicazioni di messaggistica criptata, sia l’algoritmo necessario alla

decriptazione delle comunicazioni, le quali diversamente sarebbero rimaste inintelligibili e quindi inutilizzabili in sede processuale.

Successivamente, varie Procure italiane tra cui quelle di Reggio Calabria, Milano, Genova e Napoli hanno richiesto all'autorità giudiziaria francese la messaggistica in tal modo acquisita mediante emissione di O.I.E. (Ordini di Indagine Europei), affinché fossero versati agli atti dei procedimenti instaurati in Italia i dati già in possesso dell'autorità francese.

Da tale vicenda sono, quindi, discesi plurimi problemi interpretativi che hanno investito vari aspetti attinenti sia alla qualificazione giuridica delle chat sia alla loro utilizzabilità e segnatamente:

- se la disciplina applicabile al caso di specie sia quella dell'acquisizione di documenti informatici ex art. 234-bis c.p.p. o, diversamente, quella delle intercettazioni ex artt. 266 ss. c.p.p. od ancora quella del sequestro di dati informatici ex art. 254-bis c.p.p.;
- conseguentemente, se l'O.I.E. adottato dalle Procure italiane possa essere emesso direttamente dal pubblico ministero o debba essere preceduto dall'autorizzazione del Giudice procedente ai sensi dell'art. 45 del D.lgs. 108/2017;
- se il diritto di difesa degli indagati sia da considerarsi egualmente garantito pur nell'accertata impossibilità di fornire alcuni dati in possesso dell'autorità giudiziaria francese e non comunicabili all'A.G. italiana (ad esempio, l'algoritmo di decriptazione, sul quale la Francia ha posto il segreto di Stato);
- se sia applicabile al caso di specie il generale principio di presunzione di legittimità dell'operato dello Stato esecutivo dell'O.I.E., tanto più nel caso in cui questo faccia parte dell'Unione Europea e sia tenuto al rispetto di principi sovranazionali simili a quelli cui è sottoposta l'Italia, o se il vaglio di legittimità, utilizzabilità ed ammissibilità del mezzo di ricerca della prova esperito debba essere effettuato nel caso concreto da parte del giudice italiano.

Le varie posizioni alternatesi in dottrina e in giurisprudenza sulle suddette questioni hanno quindi suscitato un dibattito giurisprudenziale, del quale sarà dato adeguatamente conto nel paragrafo che segue.

2. Il contrasto sorto nella giurisprudenza della Corte di Cassazione

Inizialmente, la giurisprudenza della Corte di Cassazione, impegnata nella risoluzione delle varie problematiche sopra elencate fin dal luglio del 2022, aveva

dato risposta di fatto univoca alle questioni interpretative che l'utilizzabilità delle chat criptate poneva.

Segnatamente, a decorrere da Sez. 1, Sentenza n. 34059 del 2022 (in senso conforme, Sez. 4, Sentenza n. 16347 del 05/04/2023 e Sez. 3, Sentenza n. 47201 del 19/10/2023) il giudice di legittimità aveva stabilito i seguenti principi di diritto.

In primo luogo, venne giudicato corretto l'assunto per il quale l'acquisizione delle chat criptate da procedimenti penali svolti all'estero potesse legittimamente avvenire mediante ricorso all'istituto dell'*Acquisizione di documenti e dati informatici* di cui all'art. 234-bis c.p.p.

In particolare, i giudici della Corte di Cassazione sottolineavano come fosse irrilevante se nel procedimento svoltosi innanzi all'A.G. francese i dati delle chat SkyEcc fossero stati acquisiti mediante attività di intercettazione o meno, giacché l'aspetto dirimente dell'intera questione era rappresentato dal fatto che, in ogni caso, le autorità italiane avevano richiesto il dato in un momento in cui l'attività captativa era già giunta a conclusione.

Da ciò, discendeva che le Procure italiane avevano richiesto il versamento in atti di un dato statico (c.d. dato freddo) che acquisiva, già sol per tale caratteristica, la natura di documento informatico ex art. 234-bis c.p.p.

Tanto, peraltro, risultava suffragato anche dalla circostanza per la quale nel modulo di emissione dell'O.I.E., inviato alle autorità francesi, non risultava compilata la sezione "H7", riservata all'*"intercettazione di telecomunicazioni"*, né la sezione "H5" relativa a *"Atti di indagine che implicano l'acquisizione di prove in tempo reale, in modo continuo e per un periodo determinato"*, ma quella relativa all'*"Acquisizione di informazioni o di prove già in possesso dell'autorità di esecuzione"* (con ciò, rilevandosi quindi che al momento di emissione dell'O.I.E. nessuna attività da svolgersi in modo dinamico o in tempo reale fosse stata richiesta dagli organi inquirenti italiani).

In ordine, poi, alla possibile lesione del diritto di difesa, veniva giudicato condivisibile l'argomento a tenore del quale potesse trovare applicazione la generale presunzione di legittimità dell'operato dello Stato estero, detta in generale dalla giurisprudenza di legittimità in tema di rogatoria internazionale (cfr. Sez. 4, Sentenza n. 19216 del 06/11/2019, dep. 2020) ed a maggior ragione ritenuta applicabile se lo Stato eseguito la richiesta di cooperazione giudiziaria fosse appartenente all'Unione Europea e, come tale, vincolato al rispetto di principi sovranazionali simili a quelli cui è sottoposto il nostro Stato.

Il suddetto principio di diritto trovava maggiore efficacia argomentativa se rapportato alle motivazioni dei provvedimenti di merito che spesso avevano finito con il rilevare, in ordine a tale aspetto, una tendenziale genericità delle doglianze difensive sollevate: infatti, frequentemente l'eccezione relativa alla lesione del diritto di difesa si risolveva in una generale critica alle modalità acquisitive delle chat criptate senza che però fossero adottati in corso di giudizio specifici argomenti da cui desumere che dalle modalità di trasmissione potesse essere disceso, in concreto, un effetto pregiudizievole per la posizione processuale del ricorrente.

Tanto più tale genericità si appalesava nel momento in cui veniva considerato dalle difese degli indagati dirimente la mancata trasmissione dell'algoritmo mediante il quale le autorità francesi e belghe erano riuscite a decriptare il contenuto delle chat, rendendole intellegibili, dato sul quale la Francia aveva posto il segreto di stato.

Un *vulnus* al diritto di difesa si sarebbe potuto, eventualmente, rilevare non dalla mancata conoscenza o conoscibilità dell'algoritmo in sé quanto dalle modalità di acquisizione di questo, comunque rese note dai plurimi provvedimenti dell'A.G. francese (segnatamente, dei Tribunali di Lille e di Parigi) versati in atti; giacché l'accoglimento della relativa doglianza difensiva avrebbe dovuto comportare un maggiore sforzo esplicativo nell'offrire una plausibile ragione per cui ritenere che il dato acquisito dall'autorità giudiziaria estera potesse essere artefatto, inventario, comunque in generale da considerarsi inattendibile a fini processuali o ingiustamente penalizzante nei confronti del ricorrente.

In ultimo, seguendo la via della qualificazione dell'atto processuale quale documento informatico ex art. 234-bis c.p.p., *ex se* nessun problema interpretativo si poneva con riguardo alla legittimità dell'O.I.E. emesso dalle Procure italiane, giacché essendo l'atto ex art. 234-bis c.p.p. di competenza del pubblico ministero, del pari quest'ultimo era da ritenersi il soggetto legittimato all'adozione del relativo O.I.E.¹

Senonché, una tale *pax* giurisprudenziale è ben presto cessata a seguito delle sentenze gemelle nn. 44154/23 e 44155/23 della Sez. 6 della Corte di Cassazione che hanno ritenuto di operare valutazioni diverse da quelle che sono state sin qui esposte.

In primo luogo, tali sentenze hanno escluso in maniera categorica che l'istituto applicabile alle chat criptate potesse essere costituito dall'art. 234-bis c.p.p. e ciò perché:

¹ In ordine a tale profilo, va ricordato che l'unica norma del D.Lgs. 21 giugno 2017, n. 108 che richiede l'autorizzazione da parte del giudice per l'adozione dell'O.I.E. è l'art. 45 in tema di Richiesta di documentazione inerente alle telecomunicazioni

- mancherebbe il legittimo consenso del titolare dei dati all'acquisizione degli stessi, presupposto dell'istituto menzionato, visto che nel caso di specie si era verificato che i dati, tanto delle chat quanto quelli da cui era stato calcolato l'algoritmo di decriptazione, erano stati acquisiti in modo indiscutibilmente occulto da parte delle autorità inquirenti francesi e quindi, di fatto, senza il consenso della Sky Global, cioè la società che tali dati deteneva;

- in ogni caso, l'art. 234-bis c.p.p. trova applicazione a documenti che sono stati formati prima o comunque fuori dal procedimento penale, mentre nel caso di specie era pacifico che l'acquisizione delle chat, la decriptazione e la relativa trascrizione in documenti digitali fosse avvenuta nel corso delle indagini svoltesi innanzi all'A.G. francese.

Pertanto, la Sesta Sezione perveniva alla soluzione di un'astratta duplice possibilità di qualificazione del materiale probatorio in atti affermando:

- che questo avrebbe dovuto essere qualificato quale *Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni* ex art. 254-bis c.p.p. nel caso in cui, all'esito dei dovuti accertamenti in sede di merito, si fosse appurato che tali dati erano stati acquisiti nella fase c.d. fredda, cioè in un momento nel quale l'intercettazione di flussi captativi era giunto al termine;

- che questo avrebbe dovuto essere qualificato quale intercettazione, regolata agli artt. 266 e seguenti c.p.p., qualora all'esito degli accertamenti di merito fosse emerso che i dati richiesti erano stati acquisiti da flussi captativi dinamici ancora in corso al momento dell'emissione dell'O.I.E. da parte delle autorità inquirenti italiane.

Appare evidente, quindi, come da tale filone giurisprudenziale possano discendere anche ulteriori profili di potenziale problematicità nell'ammettere l'utilizzabilità delle chat criptate: ad esempio, qualora l'attività captativa venisse considerata dai giudici di merito come ancora in corso al momento di adozione dell'O.I.E. (e, dunque, da qualificarsi come ex art. 266 e seguenti c.p.p.) si porrebbe il problema di dover analizzare se sussistano, nel caso di specie, i presupposti per l'utilizzabilità in altri procedimenti del materiale captativo acquisito e, cioè, se siano rispettati nel caso concreto i principi posti dall'art. 270 c.p.p. per come interpretato dalla giurisprudenza di legittimità nel nostro ordinamento².

In relazione alla problematica della legittimità dell'O.I.E. la questione è stata giudicata dalla Sesta Sezione come irrilevante nel caso di specie, giacché le difese

² Problema che, in verità, appare di scarso rilievo nei procedimenti aventi a oggetto reati in materia di stupefacenti, essendo questi delitti per cui è previsto l'arresto obbligatorio in flagranza (art. 380 c.p.p.), discendendo da ciò la possibile utilizzabilità in procedimenti diversi da quelli in cui l'intercettazione era stata disposta

dei ricorrenti non avevano contestato la legittimità dell'ordine di indagine presso lo Stato di esecuzione (cioè, in Francia) e la prova era stata ormai trasmessa all'autorità italiana.

Tale assunto vale a far ritenere irrilevante la questione sulla legittimità dell'O.I.E. nei procedimenti penali italiani già aperti ed in corso per i quali la difesa non abbia proposto opposizione nello Stato di esecuzione; ma la medesima questione finirà con l'influire in eventuali procedimenti futuri (qualora dovessero verificarsi altri casi simili di acquisizione di chat criptate) giacché se l'atto probatorio dovesse essere qualificato quale intercettazione si dovrà ritenere necessario che l'O.I.E., per essere legittimo, sia preceduto dall'autorizzazione del Giudice delle Indagini Preliminari.

Nessun problema, sotto questo profilo, si rileverebbe invece qualora l'atto probatorio fosse qualificato quale documento o documento informatico (artt. 234 e 234-bis c.p.p.) o quale sequestro di dati informatici (art. 254-bis c.p.p.) giacché, essendo nel procedimento interno competente all'acquisizione di tali atti il pubblico ministero, parimenti sussisterebbe la competenza di quest'ultimo ad adottare il relativo Ordine di Indagine Europeo senza necessità di previa autorizzazione da parte del Giudice delle indagini.

In ultimo, uno degli aspetti che allo scrivente appaiono maggiormente critici, è quello relativo all'aver richiesto tali sentenze gemelle la necessità che il vaglio di ammissibilità e legittimità dell'attività probatoria svolta all'estero sia in concreto affidata al giudice italiano, così finendo con l'attenuare il generale principio di presunzione di legittimità dell'operato dallo Stato estero sul quale si era formata una ormai unanime giurisprudenza.

Tale assunto non soltanto si pone in netto contrasto con la giurisprudenza in tema di rogatoria internazionale, a tenore della quale vige un generale principio di legittimità dell'operato dello Stato estero salvo che si rinverano in corso di giudizio elementi da cui desumere in maniera non manifestamente infondata che l'attività inquirente ivi svoltasi possa contrastare con uno o più dei principi fondamentali del processo penale italiano³, ma appare essere anche in attrito con la marcata tendenza sovranazionale, ed in particolare comunitaria, a prevedere forme sempre più stringenti di cooperazione giudiziaria, le quali trovano il loro indefettibile presupposto in un rapporto di fiducia intercorrente tra Stato richiedente e Stato eseguento gli ordini di indagine (tanto più, si ribadisce, allorché tali Stati facciano entrambi parte degli stessi organismi sovranazionali, come nel caso delle chat SkyEcc in cui Italia, Francia, Belgio ed Olanda fanno tutte parte dell'Unione

³ cfr. Sez. 4, Sentenza n. 19216 del 06/11/2019 - dep. 2020, in senso conforme Sez. 6, Sentenza n. 44882 del 04/10/2023

Europea e come tali tenuti al pedissequo rispetto dei principi di diritto e delle norme regolamentari da questa adottate).

All'esito di tale riepilogo giurisprudenziale, va poi rilevato come vi siano stati, da ultimo, ulteriori arresti della Corte di legittimità⁴, tale da fornire ulteriori possibili chiavi di lettura della questione esaminata avendo sostenuto:

- l'impossibilità di qualificare l'atto probatorio quale art. 234-bis c.p.p., giacché tale disposizione legittima l'A.G. italiana ad acquisire unilateralmente i documenti informatici e cioè senza ricorrere alle procedure di cooperazione internazionale cui si è fatto invero nel caso di specie ricorso;

- l'astratta possibilità di qualificare dunque le chat criptate acquisite dalla Francia quale documento "semplice" ex art. 234 c.p.p. suscettibile di sequestro ex art. 254-bis c.p.p.;

- la legittimità dell'O.I.E. adottato dal pubblico ministero anche senza previa autorizzazione del Giudice delle Indagini Preliminari, poiché la disciplina del sequestro ex art. 254-bis c.p.p. (la quale non è stata oggetto di alcuna pronuncia che ne sancisse il contrasto con la disciplina comunitaria, a differenza di quanto avvenuto con la sentenza HK della Corte di Giustizia dell'Unione Europea in relazione all'art. 132 D.Lgs. 196/2003, sulla quale ci si soffermerà diffusamente in seguito) prevede la possibilità che tale atto probatorio venga adottato direttamente dall'organo inquirente;

- la conferma del principio di presunzione di legittimità dell'operato dello Stato estero che può essere superato solo nel caso di violazione dei principi fondamentali della materia o nel caso di concreti elementi sollevati dalla difesa sulla base dei quali è possibile denotare il mancato rispetto delle garanzie poste a tutela della sfera giuridica dell'indagato, rilevando altresì che, in ogni caso, tale lesione del diritto di difesa non possa comunque discendere dalla mancata ostensione dell'algorithmo o delle modalità di "hackeraggio" del sistema informatico, atteso che l'ordinamento nazionale stesso, anche nei procedimenti che si basino esclusivamente su prove acquisite integralmente nello Stato, *"non obbliga alla ostensione degli attrezzi virtuali con cui si sia ottenuta la decodifica di contenuti telematici"*.

Preso atto delle varie posizioni giurisprudenziali formatesi su tali aspetti, in data 3 novembre 2023 la Sez. 3 con ordinanza n. 47798/23 (imp. Gjuzi) ha quindi rimesso la questione all'esame delle Sezioni Unite della Corte di Cassazione, ponendo i seguenti quesiti:

⁴ cfr. Sez. 6, Sentenza n. 46482 del 27/09/2023, nello stesso senso Sez. 6, Sentenza n. 46833/2023

“a) Se in tema di mezzi di prova la acquisizione di messaggi su chat di gruppo scambiati con sistema cifrato, mediante O.E.I., 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. 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.”

Parimenti, all’udienza tenutasi il successivo 15 gennaio 2024, la Sez. 6 adottava altra ordinanza di rimessione alle Sezioni Unite (ordinanza n. 2329/24, imp. Giorgi +1) di ulteriori e diverse questioni, così riassunte:

“1) Se l’acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazione disposte dall’Autorità giudiziaria estera su una piattaforma criptata integri, o meno, l’ipotesi disciplinata nell’ordinamento interno dall’art. 270 cod. proc. pen.;

2) Se l’acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte dall’Autorità giudiziaria estera mediante l’inserimento di un captatore informatico sul “server” di una piattaforma criptata sia soggetta nell’ordinamento interno a un controllo giurisdizionale, preventivo o successivo, in ordine alla utilizzabilità dei dati raccolti”.

Appare rilevante pertanto opportuno, per ragioni di completezza, esprimere un breve commento anche sull’ordinanza da ultimo menzionata.

In primo luogo, pare che dai “quesiti” di diritto formulati, la risoluzione delle questioni sia anzitutto subordinata all’eventualità che, all’esito della decisione del primo ricorso oggetto di rimessione, giacché è evidente che se l’acquisizione delle chat Sky Ecc dalla Francia non dovesse essere qualificata come attività di intercettazione, *ex se* verrebbe meno, nel caso concreto, la rilevanza dell’applicabilità o meno dell’art. 270 c.p.p. sull’utilizzazione delle captazioni in procedimento diverso (ancorché la medesima questione potrebbe trovare comunque un suo astratto rilievo, qualora in futuro dovessero esservi casi di acquisizione di contenuti di intercettazioni mediante emissione di apposito o.i.e.).

Secondariamente, l’ordinanza n. 2329/24 pare allo scrivente essere di assoluto pregio perché solleva dubbi su ulteriori aspetti, rispetto a quelli già dapprima attenzionati da altre pronunce, in ordine ai quali parimenti vi sarebbe necessità di chiarimento da parte delle Sezioni Unite della Corte di Cassazione.

In primo luogo, una questione di assoluto interesse è quella attinente al capire se risponda ai requisiti di proporzionalità del mezzo di ricerca della prova, vigente nell'ordinamento interno, considerato che nel caso di specie la Francia aveva acquisito, in maniera che le difese hanno ritenuto essere indiscriminata, le chat di decine di migliaia di utenti SkyEcc, anche nell'ipotesi di soggetti non attinti dal seppur minimo indizio di reità (sotto tale profilo, i sostenitori di una tesi più marcatamente "giustizialista" potrebbero ritenere che già il sol fatto che un soggetto utilizzasse la piattaforma SkyEcc fosse esso stesso indizio di reità, giacché diversamente dovrebbe darsi una plausibile spiegazione del motivo che potrebbe spingere un soggetto a stipulare un abbonamento elevatamente costoso per effettuare comunicazioni riservatissime se ciò non trovasse la sua probabile ragione nell'effettiva conduzione di affari illeciti, comunque non esclusivamente nell'ambito del narcotraffico).

Invero, sotto tale profilo, la Sez. 6 ha rilevato come sia dato rilevarsi una potenziale discrasia tra la disciplina delle intercettazioni del codice di rito, che non prevede la figura di una captazione *ex ante* indeterminata nei confronti di un numero imprecisato di bersagli, e quella contenuta nel d.lgs. 108/2017 (artt. 24 e 43), a tenore della quale sarebbe invece ammissibile l'intercettazione di interi sistemi informatici o telematici senza previa individuazione dei singoli bersagli.

Parimenti, dubbi ha suscitato la circostanza per la quale l'A.G. francese aveva utilizzato un *trojan* per acquisire non solo le strette comunicazioni (nel caso di specie, il contenuto delle chat) ma anche l'algoritmo di decriptazione.

Il problema sottostante è, quindi, capire se un tale utilizzo del trojan fosse contemplabile nel nostro ordinamento giuridico, essendo ammissibile l'o.i.e. solo per esperire mezzi di ricerca della prova che sono attivabili "*in un caso interno analogo*" (art. 6, par. 1 lett. b, direttiva 2014/41/UE – in sintesi, se si ritenesse che tale mezzo di ricerca della prova non fosse ammissibile nel nostro ordinamento, cioè comporterebbe problemi in ordine tanto all'utilizzabilità della prova acquisita quanto, a monte, della legittimità dell'o.i.e. emesso, proprio per potenziale contrasto con l'art. 6 direttiva 2014/41/UE).

In tal senso la Corte ha rilevato due possibili argomenti, uno a favore ed uno contrario all'ammissibilità di un tal mezzo di ricerca della prova, e segnatamente:

- a favore, che la norma ex art. 266-bis c.p.p. apparirebbe garantire adeguata copertura normativa all'attività compiuta dalle Procure nazionali, giacché potrebbe correttamente essere rilevato come, anche per captare l'algoritmo, l'attività sia

consistita sostanzialmente in una captazione di flussi comunicativi, come tale certamente attivabile anche nel nostro ordinamento;

- in senso contrario, invece, militerebbe l'argomento per il quale le stesse norme del codice di rito appaiono riferirsi esclusivamente all'ipotesi di inoculazione del trojan in dispositivo elettronico portatile, quando invece nel caso di specie esso era stato eventualmente inoculato nelle strutture immobili dei server di Roubaix.

Passando, ancora, ad un terzo ed ulteriore problema di diritto individuato dall'ordinanza n. 2329/24, questo è relativo alla questione se possa ritenersi tutelato il diritto di difesa dell'indagato pur nell'impossibilità di fornire alla difesa di quest'ultimo alcuni dati non ostensibili, quale ad esempio nel caso di specie è l'algoritmo di decriptazione delle chat.

Il problema era già stato affrontato nel corpo delle summenzionate sentenze n. 46482 del 27/09/2023 e n. 46833/2023, in senso dell'assenza di lesione del diritto di difesa, ed eppure anche tale questione viene, dall'ordinanza 2329/24, rimessa in discussione avendo, anche in questo caso, la Corte individuato ragioni a favore o contrarie all'una o all'altra tesi, per la completa lettura delle quali si fa in tal sede integrale rinvio al punto 10 dell'ordinanza 2329/24 (pagg. 29 e seguenti).

Nel corpo del presente paragrafo si è pertanto cercato di fare un'elencazione, peraltro forse nemmeno esaustiva, di tutte le questioni fin qui sollevate sulle chat criptate; sotto tale profilo, appare allo scrivente auspicabile che anche le problematiche da ultimo esposte, ancorché non specificamente contemplate nei quattro quesiti di diritto posti nelle summenzionate ordinanze di remissione, trovino soluzione nel corpo delle motivazioni delle sentenze che adotteranno le Sezioni Unite all'udienza del prossimo 29 febbraio 2024; in caso contrario, infatti, vi sarebbe il concreto pericolo che, qualora all'esito delle decisioni delle SS.UU. dovessero ancora residuare "vuoti" di chiarezza sulla corretta ricostruzione giuridica delle chat, potrebbero nell'immediato futuro ritenersi opportune, se non addirittura necessarie, ulteriori ordinanze di remissione, con conseguente perdurante protrarsi dell'intenso dibattito giurisprudenziale fin qui sintetizzato.

3. Gli elementi "esterni" rilevanti: la giurisprudenza della Corte Costituzionale e quella della Corte di Giustizia dell'Unione Europea

Così delineati i contorni generali del dibattito in atto, va detto che un'importante chiave di lettura, per una riflessione che parte dalla questione delle chat SkyEcc ma finisce con l'inglobare più in generale lo stato dell'ordinamento giuridico nazionale in tema di acquisizione di chat anche non criptate (cioè, quelle che usualmente

avvengono per il tramite dell'utilizzo di applicativi a disposizione di tutti i consociati, quali Whatsapp e Telegram per citare i due più diffusi), è altresì data dalla recente giurisprudenza sia della Corte Costituzionale che della Corte di Giustizia dell'Unione Europea.

Le posizioni assunte dalle Corti poc'anzi menzionate assumono rilevanza tanto più se si consideri che i principi di diritto contenuti nelle sentenze che saranno di seguito illustrate hanno costituito il fondamento teorico dell'elaborazione del percorso interpretativo inaugurato dalla Sesta Sezione della Corte di Cassazione, in contrapposizione a quello dapprima consolidatosi.

In primo luogo, rilevante è la sentenza della Corte Costituzionale n. 170 del 2023⁵ che ha qualificato i messaggi inviati e ricevuti tramite chat quale corrispondenza, così ritenendo necessaria l'applicazione della tutela rafforzata prevista dall'art. 15 della Costituzione (e, sotto il profilo procedurale, l'art. 254 c.p.p. in tema di sequestro di corrispondenza).

Il passaggio più interessante della sentenza in esame è quello a tenore del quale, nel nostro ordinamento giuridico, il concetto di corrispondenza *“si presterebbe infatti a ricomprendere, oltre alla tradizionale corrispondenza cartacea recapitata a mezzo del servizio postale e telegrafico (divenuta ormai «statisticamente minoritari[a]»), anche i messaggi scritti scambiati attraverso strumenti di tipo informatico e telematico: messaggi assistiti dalla medesima garanzia di segretezza, assicurata dalle credenziali di accesso riservate per la corrispondenza elettronica e dalla disponibilità esclusiva, in capo ai corrispondenti, dei dispositivi elettronici utilizzati per lo scambio dei messaggi di testo”*.

Tale interpretazione risponde pienamente, a parere dello scrivente, a un criterio basato sulla nozione semantica del termine corrispondenza: se per tale, infatti, viene individuato un messaggio scritto inviato da un mittente e ricevuto da un destinatario, connotato dai caratteri di segretezza e riservatezza, non si pone altra via che qualificare la messaggistica a mezzo chat quale corrispondenza.

Condivisibile è anche il principio, dal quale mi pare non si possa ragionevolmente dissentire, per cui non vi sarebbe plausibile e razionale motivo per non applicare la disciplina della corrispondenza, già presente nella nostra Costituzione (art. 15 Cost.) e nel nostro codice di rito (art. 254 c.p.p.), non solo a quella cartacea ma anche a quella telematica.

⁵ Per un approfondimento, si veda BORGABELLO M., Il concetto di “corrispondenza” nella sentenza 170 del 2023 della Corte costituzionale, *Giurisprudenza Penale Web*, 2023, 7-8 – ISSN 2499-846X

Senonché, i profili di criticità derivano dal fatto che tutta la disciplina posta nel nostro ordinamento giuridico nazionale è stata elaborata per un tipo di corrispondenza completamente diverso rispetto a quello attuale, avendo avuto modo la stessa Corte Costituzionale di delineare come la corrispondenza cartacea recapitata a mezzo del servizio postale e telegrafico sia ormai divenuta ben meno frequente a favore dei più avanzati e moderni metodi di interazione telematica.

In altri termini, la criticità che in questa sede vuol farsi rilevare è quella per la quale il legislatore (comprensibilmente visto che al tempo non era presente, né era immaginabile, un tipo di corrispondenza diversa da quella cartacea) ha previsto la normativa basandola su un invio episodico, occasionale, comunque non continuativo di missive cartacee; il problema per l'interprete di diritto è quindi valutare se tale disciplina, ancor oggi vigente nel codice di rito, possa ritenersi idonea a realizzare un equo contemperamento tra le esigenze di riservatezza del cittadino e quella di giustizia.

Appare evidente, infatti, come dal punto di vista sostanziale le caratteristiche della corrispondenza telematica e di quella cartacea siano nettamente differenti.

Per la rapidità, costanza e continuità che caratterizzano lo scambio di messaggi di breve lunghezza, le chat costituiscano ormai il principale mezzo di interazione tra consociati; ne consegue, pertanto, che il sequestro dei dispositivi mobili e l'acquisizione delle chat assume per l'indagato o per qualsivoglia altro soggetto caratteri di invasività molto più profonda di quella che poteva assumere il sequestro della singola o di più singole missive cartacee.

Allora, mi pare che delle due l'una: o la Corte Costituzionale avrebbe dovuto prendere atto del fatto che i messaggi via chat, per le loro menzionate caratteristiche di rapidità, costanza e continuità, assumono nella loro essenza la natura sostanziale di comunicazioni, ed allora si sarebbe dovuta applicare la relativa disciplina posta all'art. 266 ss. c.p.p. (ma è evidente come ciò avrebbe dovuto comportare una forzatura interpretativa, cioè quella di qualificare quali comunicazioni elementi che comunicazioni non sono, sol perché la relativa disciplina appare maggiormente adeguata ad assicurare il contemperamento tra privacy e giustizia cui si è dapprima brevemente accennato); oppure il legislatore, preso atto della posizione assunta dalla Giudice delle leggi e preso altresì atto dell'inidoneità dell'attuale disciplina sulla corrispondenza a garantire efficace compromesso tra esigenze di giustizia e tutela della privacy dei consociati, dovrebbe seriamente riflettere, a parere dello scrivente, sull'opportunità di una riforma del codice di rito, volta ad innovare la disciplina alla

luce delle novità tecnologiche che ormai da più di un decennio sono entrate a far parte della quotidianità di ciascuno di noi.

Peraltro, la necessità di tutelare la privacy dei cittadini in modo più deciso rispetto a quanto attualmente è previsto nella disciplina dei sequestri posta dal codice di procedura penale pare discendere altresì dalla non meno rilevante giurisprudenza formatasi in seno alla Corte di Giustizia dell'Unione Europea.

In particolare, il riferimento è alla sentenza del 2 marzo 2021, H.K., C-746/18⁶ nel corpo della quale sono stato stabiliti i seguenti relevantissimi principi di diritto:

- un primo, a tenore del quale *“L’articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, letto alla luce degli articoli 7, 8 e 11 nonché dell’articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell’Unione europea, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l’accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi all’ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull’ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, e ciò indipendentemente dalla durata del periodo per il quale l’accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo.”*;

- un secondo, a tenore del quale *“L’articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11 nonché dell’articolo 52, paragrafo 1, della Carta dei diritti fondamentali, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l’azione penale in un successivo*

⁶ Per un approfondimento, si veda ANDOLINA E., La sentenza della Corte di giustizia UE nel caso H.K. c. Prokuratuur: un punto di non ritorno nella lunga querelle in materia di data retention? / The ruling of the EU Court of Justice in the H.K. c. Prokuratuur: a tipping point in the long controversy over data retention?, in *Processo penale e giustizia* n. 5 del 2021

procedimento, competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale.”

Con tale importante decisione la C.G.U.E. sanciva in modo deciso l'incompatibilità con il diritto comunitario delle norme processuali nazionali che stabilivano:

- che i dati dei tabulati telefonici potessero acquisiti in procedimenti per reati di qualsivoglia gravità, dovendo tale intrusivo mezzo di ricerca della prova essere limitato solo alle ipotesi di contrasto alle più gravi forme di criminalità;
- che il pubblico ministero potesse *ex se* disporre l'acquisizione dei tabulati telefonici e dei dati relativi all'ubicazione degli utenti nell'ambito di procedimenti penali senza la previa autorizzazione di un giudice terzo non costituente parte processuale.

Tale decisione ha, pertanto, comportato la necessità di un'innovazione legislativa attuata con il D.L. 30 settembre 2021, n. 132 che ha modificato l'art. 132, comma 3, D.Lgs. 196/2003 (T.U. privacy) ed inserito il nuovo comma 3-bis, prevedendo:

- la necessità che l'acquisizione dei tabulati avvenga mediante adozione di “*decreto motivato del giudice su richiesta del pubblico ministero*” (salvi i casi di urgenza, in cui i tabulati possono essere acquisiti direttamente dal pubblico ministero, salva successiva convalida da parte del G.I.P., cfr. art. 132, comma 3-bis, D.Lgs. 196/03);
- la limitazione del ricorso a tale mezzo di ricerca della prova solo per alcuni reati di particolare gravità, e cioè quelli “*per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni*” e quelli “*di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi*”.

Orbene, posto che il menzionato intervento legislativo, ancorché “sollecitato” dalla giurisprudenza comunitaria formatasi in materia, appare allo scrivente assolutamente condivisibile nel garantire un migliore temperamento delle esigenze di giustizia e di tutela della privacy, non può non vedersi come simili esigenze si pongano anche nel tema delle chat e non solo in riferimento a quelle criptate oggetto della rimessione a Sezioni Unite di cui si è detto ma anche per quelle “ordinarie” utilizzate dai consociati anche non per scopi propriamente illeciti.

Si muove nello stesso senso delle tesi qui esposte anche la considerazione contenuta nella sentenza “gemella” della Sez. 6, n. 44155/23 nella parte in cui la stessa afferma che “... è possibile concludere che l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione debba essere sempre autorizzata da un giudice: sarebbe davvero singolare ritenere che per l'acquisizione dei dati esterni del traffico telefonico e telematico sia necessario un preventivo provvedimento autorizzativo del giudice, mentre per compiere il

sequestro di dati informatici riguardanti il contenuto delle comunicazioni oggetto di quel traffico sia sufficiente un provvedimento del pubblico ministero.”

In sintesi, la Suprema Corte ha rilevato come si ponga un'evidente discrasia nel ritenere necessaria l'autorizzazione del giudice per l'acquisizione dei tabulati telefonici e la medesima garanzia non sia invece prevista invece nel caso di un mezzo di ricerca della prova ancor più invasivo quale indubbiamente è l'acquisizione delle chat.

Lo scrivente ritiene pertanto che, per tutte le ragioni fin qui esposte, l'interessante dibattito giurisprudenziale instauratosi in ordine alla qualificazione giuridica e alla utilizzabilità delle chat Sky Ecc possa tramutarsi in una preziosa occasione di rivisitazione del nostro ordinamento giuridico, nel senso della previsione di un'innovativa legislazione in tema di acquisizione di chat (criptate e non) anche precedendo sul punto possibili ulteriori approdi della giurisprudenza comunitaria in un percorso che va, ormai ed inequivocabilmente, sempre più nella direzione di assicurare una maggiore e più solida tutela della privacy del cittadino, pur senza al contempo frustrare le esigenze legate alla repressione delle forme più gravi di criminalità.

4. Conclusioni e prospettive *de iure condendo*

Ed allora, riprendendo quanto affermato alla fine del paragrafo precedente, al di là dell'esito e dei principi di diritto che saranno elaborati dalle Sezioni Unite Gjuzi all'udienza del 29 febbraio 2024, mi pare che non debba andar persa l'occasione di una ancor più ampia riflessione sulla reale compatibilità della disciplina dell'acquisizione delle chat (si ribadisce, anche non criptate) con i principi nazionali e comunitari dettati dai più recenti approdi delle Corti nazionali e comunitarie.

In particolare, credo che ogni studioso del diritto processuale penale debba porsi degli interrogativi legati all'enorme differenza tra la disciplina ipergarantista posta in tema di intercettazioni e quella, ben meno restrittiva, posta in tema di acquisizione di chat, anche dopo la qualificazione delle stesse quale corrispondenza; cioè, in altri termini, bisognerebbe chiedersi se vi siano ragioni plausibili per differenziare così tanto il trattamento processuale di mezzi di ricerca delle prove dall'esperimento dei quali discende, ad opinione dello scrivente, una non dissimile violazione della riservatezza e della privacy dei consociati.

Ci troviamo, pertanto, innanzi a una situazione per la quale:

- le intercettazioni devono essere previamente autorizzate da un giudice, per un tempo limitato salvo proroghe, solo per reati di particolare gravità e fatto salvo il rispetto di specifiche norme in tema di utilizzabilità (ad esempio, l'art. 270 c.p.p.);
- il sequestro e l'acquisizione delle chat possono essere disposti direttamente dal pubblico ministero, permettono di acquisire comunicazioni private della persona per un tempo potenzialmente indefinito (cioè, lungo quanto è ampia la conservazione della memoria del dispositivo su cui le chat sono salvate), possono essere acquisite per reati di qualsivoglia gravità, non sono vincolate al rispetto di specifiche norme di utilizzabilità in procedimenti diversi.

Orbene, posto che nette sono le differenze tra l'una e l'altra disciplina, è lecito chiedersi se a tale palese differenza di garanzie (elevatissime nel caso dell'intercettazioni, ben meno solide nel caso delle chat) corrisponda effettivamente un diverso livello di intrusività del mezzo di ricerca della prova adottato.

Mi pare che in tal senso non si possa dubitare del fatto che ormai le chat siano mezzo mediante il quale i cittadini confidano particolari della propria vita, anche di natura ipersensibile (cioè attinenti alla salute, alla vita sessuale, etc.) in maniera ormai di gran lunga più frequente rispetto a quanto avvenga per via telefonica; giacché sotto tale profilo, la suddetta differenza di disciplina tra l'uno e l'altro elemento probatorio non troverebbe giustificazione alcuna, dovendo anzi le chat ricevere una forma di tutela quantomeno pari rispetto a quella delle intercettazioni⁷.

Tanto più tale discrasia appare acuita dal fatto che, mentre le intercettazioni permettono di scoprire solo il "futuro" della vita di una persona (cioè, i fatti che egli comunicherà a terzi dopo l'avvenuta autorizzazione da parte del G.I.P.), salvo che egli nelle conversazioni non dovesse far riferimento a fatti passati del suo vissuto, le chat costituiscono la scatola nera dell'esistenza di un consociato per un tempo, come detto, a ritroso in astratto indefinito e nella prassi sovente pari a svariati anni.

Ed allora pare doversi concludere che, nell'ipotesi di novella legislativa ormai a parere dello scrivente non più procrastinabile, l'aspetto forse meno preoccupante sia

⁷ Tesi sostenuta anche nel Documento approvato dalla 2° Commissione permanente del Senato della Repubblica (Giustizia) in data 20 settembre 2023 in tema di Intercettazioni, in cui alle pagg. 49-50 si legge *"Nel corso dell'indagine conoscitiva, in numerose audizioni, è stato rilevato come, mentre le captazioni godono di garanzie procedurali rilevanti e di una forte tutela della riservatezza una volta depositate nell'ADI, di analoghe tutele non gode invece il sequestro di dispositivi informatici come smartphone, tablet e pc. La materia, infatti, viene trattata con gli strumenti ordinari, attribuendosi al contenuto dei dispositivi informatici natura di documento, nonostante si tratti molto spesso di contenuti comunicativi rilevanti analoghi a quelli delle intercettazioni. Inoltre, si tratta di attività di ricerca della prova che, pur essendo particolarmente invasiva, è oggi possibile per qualunque tipo di reato, persino per le contravvenzioni, senza sottostare a condizioni di ammissibilità come quelle previste dall'articolo 266 del codice di procedura penale."*, sostenendo nella parte successiva del documento altresì la tesi di equiparare le modalità tecniche di esecuzione delle operazioni ai sensi di quanto attualmente dispone l'art. 268 c.p.p.

proprio quello legato alla necessità o meno di previa autorizzazione da parte di giudice terzo.

Tale previsione si pone come auspicabile perché richiesto dalla C.G.U.E. nel caso dei tabulati e, quindi, sarebbe una discrasia formale non prevederla anche per l'acquisizione di chat (per i motivi indicati dalla Sez. 6 sent. n. 44155/23, sopra esposti⁸) ma ciò non toglie che, anche qualora ciò non fosse previsto, in caso di sequestro probatorio del dispositivo il ricorrente potrebbe comunque esperire istanza di riesame, così realizzandosi, quantomeno a valle, un controllo giurisdizionale sulla legittimità del provvedimento acquisitivo.

Indefettibile mi pare invece un intervento legislativo volto a limitare l'acquisizione delle chat in procedimenti per reati di qualunque gravità (quindi, in ipotesi anche per le contravvenzioni bagatellari punite con la sola pena dell'ammenda) e a prevedere l'ammissibilità del detto mezzo di ricerca della prova solo nelle ipotesi di lotta alle forme più gravi di criminalità; in tal senso, mi pare che la già sostenuta tesi della pari intrusività dell'acquisizione delle chat rispetto alle intercettazioni possa suggerire un "ricopiare" per il sequestro dei dispositivi il catalogo dei reati per i quali sono ammissibili le intercettazioni ai sensi dell'art. 266 c.p.p.

In ultimo, sarebbe auspicabile: l'introduzione di un'ipotesi di regime di utilizzabilità in altri procedimenti delle chat acquisite, potendo anche in questo caso ritenersi astrattamente applicabili le norme e gli approdi giurisprudenziali adottati in tema di intercettazione, e quindi in sostanza relativi all'art. 270 c.p.p.; la previsione di un limite temporale a ritroso di acquisizione delle chat, ad esempio parametrandolo al *tempus commissi delicti* oggetto di contestazione; la previsione di un regime transitorio volto ad evitare l'inutilizzabilità delle chat acquisite prima dell'entrata in vigore della qui prospettata riforma.

Sulla scorta di tutto quanto fin qui esposto credo, in conclusione, che l'interessante dibattito giurisprudenziale venutosi a creare, al di là dell'approdo delle Sezioni Unite cui la giurisprudenza di merito si uniformerà in tema di chat criptate Sky Ecc, possa costituire grande occasione per rendere, in ordini a tali profili ormai al centro del contesto europeo ed internazionale, il nostro ordinamento innovativo, all'avanguardia e maggiormente adeguato a costituire garanzia nei confronti di tutte le parti processuali in riferimento alle problematiche che il tempo attuale ci pone.

⁸ "... sarebbe davvero singolare ritenere che per l'acquisizione dei dati esterni del traffico telefonico e telematico sia necessario un preventivo provvedimento autorizzativo del giudice, mentre per compiere il sequestro di dati informatici riguardanti il contenuto delle comunicazioni oggetto di quel traffico sia sufficiente un provvedimento del pubblico ministero"

Quanto rilevato nel corso della presente trattazione tende pertanto a indicare come, a parere dello scrivente, l'approdo delle Sezioni Unite in tema di qualificazione giuridica ed ammissibilità delle chat criptate Sky Ecc costituirà certo un importante momento di confronto dal quale trarre ulteriori spunti di riflessione nella complicata materia esaminata ma esso dovrebbe costituire un punto di partenza e non di arrivo; l'auspicio è, infatti, rappresentato dall'ideazione ed attuazione di una disciplina chiara, univoca e aggiornata che sia idonea a costituire garanzia per tutte le parti processuali, e particolarmente per l'indagato, e che indichi con chiarezza il percorso ermeneutico da seguire nell'acquisizione di conversazioni telematiche che sempre più assumono rilevanza nell'ambito del processo penale odierno, all'insegna dell'eterno compromesso da ricercarsi tra le esigenze di giustizia e la necessaria tutela della privacy del cittadino.