Numero 4 - 2024

L'utilizzabilità delle *chat* criptate acquisite mediante ordine europeo di indagine

The usability of encrypted chats acquired through the European Investigation Order

Maria Luisa Miranda

Abstract [It]: il saggio si sofferma sul tema dell'utilizzabilità nel processo penale di dati oggetto di conversazioni criptate con particolare riferimento alla disciplina dell'ordine europeo d'indagine.

Abstract [En]: *the paper focuses on the issue of the usability of data from encrypted conversations in criminal proceedings with particular reference to the regulation of the European Investigation Order.*

Parole chiave: processo penale - prove.

Keywords: *criminal law proceeding - evidence*.

1. Premessa.

Lo sviluppo delle tecnologie informatiche e delle modalità di comunicazione per via telematica ha comportato un palpabile miglioramento per l'intera collettività, permettendo una maggiore rapidità e semplicità di comunicazione ma, al contempo, un massiccio impiego di tali avanzate strumentazioni, anche da parte delle organizzazioni criminali, ha generato una sempre più diffusa globalizzazione del crimine.

Le più recenti attività investigative, condotte da diverse Procure di Stati europei, hanno infatti appurato come, per il tramite dell'utilizzo di cellulari dotati di applicazioni denominate "*EncroChat*" e "*Sky-Ecc*", vari soggetti impegnati in attività criminali, specialmente nel settore del narcotraffico transazionale, siano riusciti, in maniera del tutto indisturbata, a organizzare l'importazione, la detenzione e la successiva commercializzazione in Europa di ingentissime quantità di stupefacente, prevalentemente del tipo cocaina, approdate attraverso i porti europei di Gioia Tauro, Anversa e Rotterdam, provenienti dal Sud America.

 Copyright © - www.quotidianolegale.it

Numero 4 - 2024

A tali risultati investigativi si è giunti attraverso vari *step*. Nell'anno 2016, la Polizia del Belgio e quella dell'Olanda hanno avviato un'indagine nei confronti della società canadese Sky Global, la quale, tramite cellulari criptati e l'utilizzo dell'applicazione *Sky-Ecc,* ha fornito soluzioni di crittografia PGP basata su un'infrastruttura di comunicazione dedicata.

Accertato l'uso diffuso della soluzione telefonica crittografata tra le reti criminali internazionali di tutto il mondo, nel 2019, le autorità francesi decidevano di aprire un caso presso *Eurojust*, l'Agenzia dell'UE per la cooperazione giudiziaria penale. I dati, acquisiti con autorizzazione giudiziaria[1] sulla base delle disposizioni del diritto francese, venivano condivisi in prima istanza con i Paesi Bassi, mediante la creazione di una *Squadra Investigativa Comune* (Francia e Olanda), con la partecipazione, dall'aprile 2020, di *Europol*, l'Agenzia dell'Unione europea per la cooperazione tra le forze dell'ordine.

A metà del mese di giugno 2020, con una prima operazione denominata "Emma95", la costituita squadra investigativa francese, olandese e belga e le rispettive Autorità giudiziarie, penetrano il sistema crittografato *EncroChat*, riuscendo a decifrare molteplici messaggi. Sulla base dei dati acquisiti, le forze dell'ordine dei diversi Paesi, con il supporto di *Eurojust*, eseguono oltre ottocento arresti, sequestrano più di dieci tonnellate di stupefacente e recuperano un centinaio di armi da fuoco.

Successivamente alla decrittazione della piattaforma *EncroChat*, è stata creata una squadra investigativa comune, composta da forze di polizia olandesi, francesi e belghe, nel cui ambito sono state decrittate le comunicazioni effettuate su un'altra piattaforma di messaggistica criptata, denominata *Sky-Ecc*, sulla quale erano transitati gran parte degli utenti *EncroChat*, a seguito della pubblicazione sugli organi di stampa, nel luglio 2020, della decrittazione di quest'ultima.

Nel mese di marzo 2021, sempre le Autorità francesi, belghe e olandesi, sviluppano un'indagine internazionale su larga scala denominata "Argus". Questa volta la piattaforma presa di mira è, appunto, quella denominata *Sky-Ecc*.

Anche in questo caso, dopo aver violato i *server* (sempre allocati in Francia), si riesce ad acquisire e decriptare centinaia di milioni di messaggi scambiati tra i diversi utenti in tutto il mondo, operazione dalla quale scaturiscono, anche in questo caso, numerosi arresti e sequestri (di droga, armi e denaro)[2].

---

[1] *Tribunal Judiciaire De Lille – Juridiction Inter-Regionale Specialisee Dans La Criminalitè Organisèe* (*JIRS*).

[2] Il *Conseil Costitutionnel* (riferito sia a *EncroChat*, sia a *Sky-Ecc*) con la decisione n. 2022-987 QPC dell'8 aprile 2022, esprimendosi su una questione prioritaria di costituzionalità sollevata dalla Camera Penale della *Cour de Cassation*, ha confermato la conformità costituzionale dell'articolo 706-102-1 del codice di procedura penale con riferimento all'articolo 230-1 del medesimo codice di rito francese, che consentono al *Procureur de la République*, nel corso dell'indagine, e al giudice istruttore, in fase d'istruzione, di avvalersi dei mezzi dello Stato sottoposto al segreto di difesa nazionale per svolgere le operazioni tecniche necessarie

 Copyright © - www.quotidianolegale.it

Gli Uffici di Procura italiani entrano in possesso della messaggistica (già) de-criptata attraverso l'emissione di molteplici Ordini d'Indagine Europei, mediante cui si chiede all'Autorità giudiziaria francese, per il tramite di *Eurojust* (che verifica l'effettiva presenza nel *data-base* dei codici IMEI), di trasmettere i messaggi scambiati tra specifici codici identificativi.

L'acquisizione della messaggistica dà origine, a partire dall'anno 2022, ad una moltitudine di procedimenti penali ed all'emissione di un indefinito numero di ordinanze cautelari, su tutto il territorio nazionale.

2. Il funzionamento dei sistemi di comunicazione crittografati.

Prima di procedere oltre non si può, però, prescindere da una pur sommaria descrizione del meccanismo di funzionamento dei "criptofonini", nella specie, quelli operanti sulla già citata piattaforma *Sky-Ecc*, gestita dalla società canadese Sky Global.

Essa utilizza sofisticati metodi crittografici a più livelli di sicurezza, attivi sia sui dispositivi mobili, sia sui *server* intermediari, per resistere ai tentativi di intercettazione.

Si tratta, dunque, di "criptofonini anti-intercettazione", da intendersi come *smartphone* che impiegano un *hardware standard* (in genere *Apple*, *Android* o *Black Berry*), ma che, rispetto agli apparecchi mobili tradizionali, si connotano per l'installazione di un'apposita scheda SIM e di un sistema operativo dedicato, avente particolari requisiti di sicurezza, in quanto disabilita i servizi di localizzazione (GPS, *Bluetooth*, fotocamera, scheda SD e porta USB).

Le chiamate rimangono attive solo in modalità *Voice over IP* (*VoiP*), non avvalendosi della rete GSM, ed impiegano applicazioni di cui sono proprietarie le piattaforme stesse[3] (*EncroChat*, *Sky-Ecc*, *Anom*, e così via), che utilizzano reti diverse dalla normale rete telefonica, e che sono crittografate ad una cifratura a più livelli.

I *backup* delle comunicazioni vengono invece salvati sul dispositivo criptato e su di un *server* dedicato messo a disposizione degli utenti dell'impresa che fornisce il servizio. Anche la SIM utilizzata è particolare e dedicata, connettendosi esclusivamente alla rete di *server* predisposta dal fornitore del servizio. In tal modo i criptofonini sarebbero al sicuro da intercettazioni.

all'acquisizione e all'estrapolazione dei dati, con l'effetto di schermare le informazioni relative a tali mezzi dal contraddittorio.

[3] Vedi memoria del Procuratore Generale, presso la suprema Corte di cassazione, per l'udienza innanzi alle Sezioni Unite Penali del 29 febbraio 2024 nel procedimento recante n.R.g. 33544/2023.

 Copyright © - www.quotidianolegale.it

Gli *smartphone* modificati vengono venduti con applicazioni preinstallate, tra cui una di messaggistica basata su *OTR* (*off-the-record* è un protocollo che fornisce la crittografia per le conversazioni di messaggistica istantanea), ed un servizio di chiamata vocale basato su *ZRTP* (*Z-Real-Time-Transport-Protocol*, ovverosia un protocollo che consente di effettuare chiamate criptate su rete *internet*).

Il sistema *Sky-Ecc* utilizza questa tecnologia. L'applicativo garantisce la sicurezza delle informazioni in questo modo: alla prima attivazione del dispositivo si generano le chiavi private (la *master key*) per la cifratura *end-to-end*; una volta inserita la *password* di sblocco il dispositivo verifica la sicurezza della connessione al *server* (se vengono riscontrati problemi di sicurezza non è possibile utilizzare il sistema di messaggistica *Sky-Ecc*); all'esito positivo della verifica della sicurezza della connessione avviene lo scambio di chiavi e la successiva procedura di autenticazione al *server*; terminate queste fasi l'utente può iniziare a scambiare i messaggi di testo e a condividere i propri *file* multimediali.

Rispetto ai primi apparecchi criptati, la piattaforma *Sky-Ecc* prevede, inoltre, ulteriori forme di "protezione", quali: la cancellazione automatica dei messaggi dopo trenta secondi; la conservazione del messaggio non recapitato per un massimo di quarantotto ore nel *server* (i cd. messaggi "autodistruttivi"); il cd. "*kill switch*", mediante cui si inserisce una *password* di panico che cancella l'intero contenuto del telefono; le SIM utilizzate sui propri dispositivi sono registrate e di proprietà della piattaforma, non consentendo così di risalire all'utente; in ogni caso, nessun messaggio sarà mai conservato sul *server* per più di quarantotto ore. L'applicazione *Sky-Ecc*, dunque, è composta da diversi moduli (PGP-e-mail, ECC-e-mail, ECC-*chat*) che danno la possibilità di utilizzare memo vocali, *chat* di gruppo, invio di immagini, e-mail, chiamate vocali, immagini e messaggi autodistruggenti protetti da crittografia.

L'applicazione *EncroChat*, invece, garantisce l'anonimato degli utenti, non essendoci nessuna associazione tra il dispositivo o la SIM card e l'*account* del cliente. Il cellulare è dotato di un doppio sistema operativo, con l'interfaccia crittografata nascosta, in modo da non essere rilevabile, con limitazioni sulle funzioni della fotocamera, microfono, GPS e porta USB. I messaggi scambiati su detta piattaforma risultano crittografati con diversi livelli di cifratura. Il sistema, inoltre, dispone di una serie di funzioni, sviluppate per consentire agli utenti, in caso di sequestro del *device* da parte della polizia giudiziaria, di cancellare rapidamente, anche da remoto, i dati compromettenti presenti sul telefonino. Ad ogni utente viene associato un *nickname* per identificarsi sulla piattaforma criptata.

In tali piattaforme criptate il servizio di comunicazione si attua attraverso l'uso di telefoni appositamente adattati per il solo utilizzo dell'APP di *chat EncroChat* ovvero *Sky-Ecc* mediante

 Copyright © - www.quotidianolegale.it

l'eliminazione di ogni applicazione preinstallata e caricamento di specifici *software* o APP di crittografia, attraverso la quale gli utenti possono scambiare messaggi crittografati da un identificatore o codice PIN *Sky-Ecc* anonimo[4].

Questi "telefoni" possono essere acquistati con un abbonamento di sei mesi, trascorsi i quali dovrà essere sottoscritto un nuovo abbonamento sempre per un periodo massimo di sei mesi.

Attraverso la decrittazione delle piattaforme *EncroChat* e *Sky-Ecc*, ritenute dagli utilizzatori inespugnabili, la squadra comune formata da forze di polizia francese, belga e olandese è riuscita ad accedere e decriptare le *chat* di oltre 70.000 utenti provenienti da diversi Paesi.

3. Gli orientamenti giurisprudenziali e la rimessione delle questioni alle Sezioni Unite.

L'acquisizione della messaggistica criptata, come anticipato, ha dato origine ad una moltitudine di procedimenti penali su tutto il territorio nazionale, generando molteplici questioni poste all'attenzione, dapprima dei giudici di merito e, successivamente, a quelli di legittimità, questioni poi sfociate nelle note ordinanze di rimessione alle Sezioni Unite.

È necessario, però, operare un breve *excursus* storico, anche per meglio comprendere le condivisibili decisioni assunte dalle Sezioni Unite che, con le pronunce del 29 febbraio 2024, hanno fatto luce su numerose questioni, fissando fondamentali principi di diritto.

Nel solco di un primo filone interpretativo, formatosi in seno alla suprema Corte all'indomani delle prime pronunce di merito, si è sostenuta la possibilità di acquisire le *chat* criptate ai sensi dell'art. 234-*bis* c.p.p. (che consente l'acquisizione di documenti e dati informatici conservati all'estero), delineando una distinzione tra le intercettazioni, da un lato, e le attività di acquisizione e decifrazione di dati comunicativi dall'altro[5].

Tale orientamento distingue tra l'operazione di captazione del messaggio cifrato in transito verso il destinatario e le operazioni di acquisizione e decriptazione del contenuto inoltrato, ritenendo applicabile solo al primo caso la disciplina delle intercettazioni, in quanto flussi di comunicazioni *ex* art. 266-*bis* c.p.p. I messaggi ormai inviati e ricevuti, diversamente, rappresenterebbero una mera

[4] M. RAMPIONI, *I limiti di utilizzabilità della messaggistica criptata* Sky-Ecc *acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali*, in *www.giurisprudenzapenale.com*, 25 ottobre 2023.
[5] In tal senso, Cass., Sez. IV, 30 maggio 2023, n. 37503; Cass., Sez. IV, 16 maggio 2023, n. 38002; Cass., Sez. IV, 9 maggio 2023, n. 23999; Cass., Sez. IV, 18 aprile 2023, n. 19969; Cass., Sez. IV, 4 aprile 2023, n. 18514; Cass., Sez. IV, 5 aprile 2023, n. 16345; Cass., Sez. IV, 5 aprile 2023, n. 16347; Cass., Sez. I, 13 ottobre 2022, n. 6364.

 Copyright © - www.quotidianolegale.it

documentazione di tali flussi comunicativi, utilizzabili come prova allorquando vi fosse la disponibilità della chiave crittografica che consentisse di decifrarne il tenore.

Sulla base di tale distinzione tra dati "*in itinere*" e dati "cristallizzati" sulla memoria di un dispositivo, la giurisprudenza citata ha ritenuto possibile l'acquisizione di questi ultimi tramite un ordine europeo d'indagine (OEI) attivato dal Pubblico Ministero[6].

L'art. 234-*bis* c.p.p. rappresenta, secondo questa impostazione, la norma interna che attribuisce il potere necessario per procedere con l'OEI, che può essere utilizzato qualora i medesimi atti di indagine richiesti «*avrebbero potuto essere emessi in un caso interno analogo*» (Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014).

La giurisprudenza in disamina ha sostenuto che nessun controllo deve essere effettuato dal Giudice italiano rispetto alla prova acquisita nell'ambito del procedimento giurisdizionale estero, sulla base del presupposto che l'attività di acquisizione sia e debba essere eseguita secondo la legislazione dello Stato estero, in quanto svolta di propria iniziativa e non su richiesta dell'A.G. italiana.

Pertanto, la tutela giurisdizionale rispetto a tale attività potrebbe essere rinvenuta solo nell'ambito dell'ordinamento estero.

A fronte di tale indirizzo, due sentenze della Cassazione – una successiva all'altra – hanno dato luce ad un orientamento difforme.

In particolare, con queste due pronunce[7] la Corte ha sostenuto come l'acquisizione *ex* art. 234-*bis* c.p.p. sia giustificata nel caso di «*elementi informativi "dematerializzati", che preesistevano rispetto al momento dell'avvio delle indagini da parte dell'autorità giudiziaria francese ovvero che erano stati formati al di fuori di quelle investigazioni*», ma così non è stato al momento della richiesta e trasmissione dei dati in parola.

Nella prospettiva di questo secondo orientamento, un'acquisizione di questo genere dovrebbe essere inquadrata, diversamente, nell'ambito delle norme in materia di perquisizioni e sequestri ai sensi dell'art. 254-*bis* c.p.p.

---

[6] L'ordine europeo di indagine, previsto dalla Direttiva 2014/41/UE, attuata in Italia con d.lgs 21 giugno 2017, n. 108, è uno strumento di cooperazione giudiziaria in materia penale tra gli Stati membri, volto all'acquisizione transazionale di prove, anche già formate dallo Stato estero di esecuzione, e di atti investigativi. L'OEI è basato sul principio del riconoscimento reciproco, ovverosia sulla circostanza che l'autorità estera è tenuta a riconoscere e a garantire l'esecuzione della richiesta avanzata dallo Stato richiedente, con le stesse modalità previste dalla disciplina dettata nello Stato di esecuzione. I presupposti necessari per poter adottare un ordine europeo di indagine sono che l'atto investigativo richiesto all'autorità giudiziaria estera sia necessario, proporzionato e infine consentito in casi analoghi nello Stato richiedente.

[7] Cass., Sez. VI, 26 ottobre 2023, n. 44155; Cass., Sez. VI, 26 ottobre 2023, n. 44154.

 Copyright © - www.quotidianolegale.it

In aggiunta e in relazione alla questione riguardante l'OEI, l'indirizzo *de quo* reputa, inoltre, necessario verificare «*ai fini di utilizzabilità dei dati informativi acquisiti, concernenti comunicazioni nella fase "statica", se sussistevano le condizioni originarie per l'autorizzabilità in sede giurisdizionale delle relative attività investigative oggetto degli ordini europei*».

Tale orientamento, inoltre, richiama le recenti pronunce della Corte EDU[8] che hanno esteso la protezione dell'art 8 CEDU (Diritto al rispetto della vita privata e familiare) ai messaggi inviati e ricevuti tramite *internet*, nonché i principi espressi dalla Corte costituzionale con la sentenza Corte cost., 27 luglio 2023, n. 170 rispetto all'estensione delle garanzie dell'art. 15 della Costituzione ad ogni forma di comunicazione.

L'arresto interpretativo in disamina valorizza, peraltro, l'introduzione in via d'urgenza delle disposizioni di cui all'art. 132 d.lgs. 30 giugno 2003, n. 196 (c.d. "Codice della *privacy*, come modificato dal d.l. 30 settembre 2021, n. 132, convertito con modificazioni dalla l. 23 novembre 2021, n. 178), con cui il legislatore ha recentemente scelto di giurisdizionalizzare la procedura di acquisizione dei dati esterni di traffico telefonico e telematico nel procedimento penale, che adesso necessita di un provvedimento autorizzatorio motivato del giudice.

Per un terzo ed ultimo orientamento[9], infine, alla luce della pronuncia Corte cost. n.170/2023 cit., la natura di corrispondenza della messaggistica informatica (anche quando conservata dopo la ricezione) escluderebbe l'applicabilità dell'art. 234-*bis* c.p.p., rientrando invece nell'ambito dell'acquisizione di prove documentali ai sensi dell'art. 234 c.p.p.[10]

Alla luce di tale incertezza interpretativa, la III Sezione della Cassazione, con l'ordinanza del 3 novembre 2023, n. 47798, ha rimesso, allora, alle Sezioni Unite le questioni riguardanti la disciplina applicabile per l'acquisizione di *chat* criptate dall'estero (*Sky-Ecc*) e la necessità di una verifica di legittimità di tale acquisizione da parte dell'Autorità giurisdizionale italiana, ponendo le seguenti questioni: «*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 c.p.p. 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 c.p.p. o sia riconducibile in altra disciplina relativa*

[8] Corte EDU, Grande Camera, 5 settembre 2017, Barbulescu c. Romania, § 72; Corte EDU, Quinta Sezione, 17 dicembre 2020, Saber c. Norvegia, § 48. In precedenza, anche Corte EDU, Quarta Sezione, 3 aprile 2007, Copland c. Regno Unito, § 41.
[9] Cass., Sez. VI, 21 novembre 2023, n. 46833; Cass., Sez. VI, 17 novembre 2023, n. 46482.
[10] Cass. n. 46833/2023 cit.

 Copyright © - www.quotidianolegale.it

all'acquisizione di prove; *b) se 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*».

Successivamente, anche la VI Sezione della suprema Corte, con l'ordinanza del 15 gennaio 2024, n. 2329 ha rimesso alle Sezioni Unite questioni analoghe, sempre ai sensi dell'art 618, comma 1, c.p.p., formulando i seguenti quesiti: «*1) se l'acquisizione mediante ordine europeo di indagine dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera su una piattaforma informatica criptata integri l'ipotesi disciplinata nell'ordinamento interno dall'art 270 c.p.p.; 2) se l'acquisizione mediante ordine europeo di indagine dei risultati di intercettazioni da un'autorità giudiziaria straniera attraverso l'inserimento di un captatore informatico sui* server *di una piattaforma criptata sia soggetta nell'ordinamento interno a un controllo giurisdizionale, preventivo o successivo, in ordine alla utilizzabilità dei dati raccolti*».

4. La decisione delle Sezioni Unite.

Le Sezioni Unite Penali della Corte di cassazione, con le sentenze n. 23755 e n. 23756, entrambe del 29 febbraio 2024 ed entrambe depositate in data 14 giugno 2024 (cd. "decisioni gemelle"), hanno dato risposta ai summenzionati quesiti, in termini positivi quanto all'utilizzabilità dei dati acquisiti, fissando i seguenti principi di diritto: «1. *La trasmissione, richiesta con ordine europeo di indagine, del contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, non rientra nell'ambito di applicazione dell' art. 234*-bis *c.p.p., 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. c.p.p. 2. In materia di ordine europeo di indagine, le prove già in possesso delle autorità competenti dello Stato di esecuzione possono essere legittimamente richieste ed acquisite dal pubblico ministero italiano senza la necessità di preventiva autorizzazione da parte del giudice del procedimento nel quale si intende utilizzarle. 3. L'emissione, da parte del pubblico ministero, di ordine europeo di indagine diretto ad ottenere il contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, non deve essere preceduta da autorizzazione del giudice italiano, quale condizione necessaria a norma dell'art. 6 Direttiva 2014/41/UE, perché tale autorizzazione, nella disciplina nazionale relativa alla*

 Copyright © - www.quotidianolegale.it

circolazione delle prove, non è richiesta per conseguire la disponibilità del contenuto di comunicazioni già acquisite in altro procedimento. 4. La disciplina di cui all'art. 132 d.lgs. n. 196/2003, relativa all'acquisizione dei dati concernenti il traffico di comunicazioni elettroniche e l'ubicazione dei dispositivi utilizzati, si applica alle richieste rivolte ai fornitori del servizio, ma non anche a quelle dirette ad altra autorità giudiziaria che già detenga tali dati, sicché, in questo caso, il pubblico ministero può legittimamente accedere agli stessi senza chiedere preventiva autorizzazione al giudice davanti al quale intende utilizzarli. 5. L'utilizzabilità del contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, e trasmesse sulla base di ordine europeo di indagine, deve essere esclusa se il giudice italiano rileva che il loro impiego determinerebbe una violazione dei diritti fondamentali, fermo restando che l'onere di allegare e provare i fatti da cui inferire tale violazione grava sulla parte interessata. 6. L'impossibilità per la difesa di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per criptare il testo delle stesse non determina una violazione dei diritti fondamentali, dovendo escludersi, salvo specifiche allegazioni di segno contrario, il pericolo di alterazione dei dati in quanto il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, ed una chiave errata non ha alcuna possibilità di decriptarlo anche solo parzialmente».

Le Sezioni Unite aderiscono, dunque, al terzo orientamento tra quelli in precedenza indicati, ma con alcune precisazioni di cui è necessario dare atto[11].

In primo luogo, il supremo Consesso chiarisce che, con riferimento all'acquisizione, effettuata mediante OEI, di messaggi scambiati su *chat* di gruppo per mezzo di un sistema cifrato e già a disposizione dell'autorità giudiziaria straniera, non è applicabile la disciplina di cui all'art. 234-*bis* c.p.p., perché la stessa è alternativa e incompatibile rispetto a quella dettata in tema di OEI.

L'art. 234-*bis* c.p.p., che testualmente prevede «*É 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*», non disciplina, infatti, un mezzo di prova, bensì una modalità di acquisizione di particolari tipologie di elementi di prova presenti all'estero, che viene attuata in via "diretta" dall'autorità giudiziaria italiana e prescinde da qualunque forma di collaborazione con le autorità dello Stato in cui tali dati sono custoditi.

[11] A. ACETO, Sky-Ecc *e criptofonini: le prime risposte delle Sezioni Unite*, in *www.altalex.com*, 20 giugno 2024.

 Copyright © - www.quotidianolegale.it

Anche l'OEI regola una modalità di acquisizione degli elementi di prova "transfrontalieri", che si realizza, però, nell'ambito dei rapporti di collaborazione tra autorità giudiziarie di Stati diversi, tutti membri dell'Unione Europea.

Trattasi, dunque, di discipline che si riferiscono a vicende tra loro diverse in relazione al presupposto di applicazione: l'art. 234-*bis* c.p.p. riguarda l'acquisizione di elementi conservati all'estero che prescinde da forme di collaborazione con l'autorità giudiziaria di altro Stato; la disciplina relativa all'OEI pure concerne l'acquisizione di elementi conservati all'estero, da ottenere o ottenuti, però, con la collaborazione dell'autorità giudiziaria di altro Stato, con conseguente inoperatività, in tale ultimo caso, dell'art 234-*bis* c.p.p.

Ciò posto, le Sezioni Unite, con le sentenza in disamina, affermano, poi, che la Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014, relativa all'OEI, da un lato «*assegna alla disciplina da essa dettata una funzione di preminenza, in materia di acquisizione delle prove nell'ambito di rapporti di collaborazione tra autorità giudiziarie di più Stati dell'Unione Europea*», e dall'altro la stessa esprime chiaramente la volontà di regolare in modo organico il sistema di acquisizione delle prove mediante la collaborazione tra stati, come si evince dagli artt. 1 e 3 e dai Considerando (6), (7) e (35).

L'art. 1 chiarisce, infatti, che l'OEI può riguardare anche «*prove già in possesso delle autorità competenti dello stato di esecuzione*», laddove al successivo art. 3 è precisato che l'OEI medesimo si «*applica a qualunque atto di indagine, tranne all'istituzione di una squadra investigativa comune*».

Occorre, allora, rilevare che il principio di completezza della disciplina dell'OEI non è in alcun modo derogato dall'ordinamento italiano.

L'art. 1 d.lgs 21 giugno 2017, n. 108, rubricato proprio «Norme di attuazione della direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 relativa all'ordine di indagine penale» statuisce, infatti, espressamente che «*il presente decreto attua nell'ordinamento interno la direttiva 2014/41/UE del Parlamento europeo del Consiglio del 3 aprile 2014*», mentre ai sensi del successivo art. 2, comma 1, lett. a), l'ordine europeo di indagine può essere emesso anche «*per acquisire informazioni o prove che sono già disponibili*».

Individuate, quindi, le linee guida nella Direttiva 2014/41/UE e nel decreto legislativo n. 108/2017, è necessario, ora, esaminare quali sono le regole generali di tale sistema normativo.

Al riguardo, le Sezioni Unite, chiarendo che solo se l'OEI è stato legittimamente emesso, gli elementi acquisiti - per il suo tramite - potranno essere validamente utilizzati nel procedimento o nel processo pendente in Italia, evidenziano la laconicità delle disposizione interne a carattere generale, nella misura in cui da un lato, l'art 27, comma 1, del d.lgs. n. 108/2017 si limita a prevedere che «*il*

 Copyright © - www.quotidianolegale.it

pubblico ministero e il giudice che procede possono emettere, nell'ambito delle relative attribuzioni, un ordine di indagine e trasmetterlo direttamente all'autorità di esecuzione», dall'altro l'art 1 del medesimo decreto stabilisce che detto atto «*attua nell'ordinamento interno la direttiva 2014/41/UE*».

Il supremo Consesso soggiunge, però, che proprio «*la precisazione di carattere generale contenuta nell'art. 1 d.lgs. citato, induce a ritenere applicabili anche agli OEI emessi dall'autorità giudiziaria italiana le condizioni di ammissibilità previste dall'art. 6, paragrafo 1, Direttiva 2014/41/UE*», ai sensi del quale che l'autorità richiedente «*può emettere un OEI solamente quando ritiene soddisfatte le seguenti condizioni: a) l'emissione dell'OEI è necessaria e proporzionata ai fini del procedimento di cui all'art. 4, tenendo conto dei diritti della persona sottoposta a indagini o imputata; b) l'atto o gli atti di indagine richiesti nell'OEI avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo*».

Con riferimento alla sussistenza della prima condizione (necessità e proporzionalità), il relativo giudizio deve essere compiuto avendo riguardo al procedimento nel cui ambito è emesso l'ordine europeo di indagine, come inequivocabilmente desumibile dall'art. 4 della Direttiva 2014/41/UE e dal Considerando (11) della medesima direttiva; trattasi, quindi, di una valutazione da effettuarsi in concreto, rapportata allo specifico procedimento nel cui contesto è stato emesso l'OEI. Quanto, invece, alla seconda condizione (ammissibilità dell'atto richiesto alle stesse condizioni in un caso interno analogo), il giudizio circa la sussistenza della medesima presuppone l'individuazione del "tipo" di atto oggetto di OEI, postulando, pertanto, una valutazione in astratto, logicamente preliminare rispetto al giudizio inerente alla prima condizione.

Per quanto, invece, attiene alla fase di esecuzione dell'OEI, in forza del coordinamento normativo tra il d.lgs. n. 108/2017 e la Direttiva 2014/41/UE, le Sezioni Unite affermano che, ai fini dell'utilizzabilità di atti acquisiti dall'autorità giudiziaria italiana mediante l'OEI, «*è necessario garantire il rispetto dei diritti fondamentali previsti dalla Costituzione e dalla Carta dei diritti fondamentali dell'Unione Europea, e, tra questi, del diritto di difesa e della garanzia di un giusto processo, ma non anche l'osservanza, da parte dello Stato di esecuzione, di tutte le disposizioni previste dall'ordinamento giuridico italiano in tema di formazione ed acquisizione di tali atti*».

Da un lato, infatti, sia la Direttiva 2014/41/UE, in particolare agli artt. 1 e 14, sia il d.lgs. n. 108/2017, segnatamente all'art. 1, evidenziano, come principio generale, l'esigenza di assicurare il rispetto dei diritti fondamentali, e, tra questi, i diritti della difesa e ad un giusto processo.

Dall'altro, però, «*né l'art. 36 d.lgs. n. 108/2017, né altre disposizioni del medesimo decreto o della Direttiva 2014/41/UE prevedono, ai fini dell'utilizzabilità degli atti formati all'estero, la necessità di una puntuale applicazione di tutte le regole che l'ordinamento giuridico italiano fissa, in via*

 Copyright © - www.quotidianolegale.it

ordinaria, per la formazione degli atti corrispondenti formati sul territorio nazionale». In tale prospettiva, a ben considerare, è l'art. 14, par. 7, Direttiva 2014/41/UE che, imponendo allo Stato di emissione di rispettare i diritti della difesa e di garantire un giusto processo nel valutare le prove acquisite tramite l'OEI, stabilisce che sono «*fatte salve le norme procedurali nazionali*» (dizione, quest'ultima, riferita allo Stato di esecuzione).

Tale soluzione, del resto, è in perfetta linea con la costante e consolidata elaborazione giurisprudenziale secondo cui, in tema di rogatoria internazionale, trovano applicazione le norme processuali dello Stato in cui l'atto viene compiuto, con l'unico limite che la prova non può essere in contrasto con i principi fondamentali dell'ordinamento giuridico italiano e con il diritto di difesa.

Ebbene, le Sezioni Unite rimarcano, quindi, che, nell'ottica dell'accertamento del rispetto dei diritti fondamentali, assumono rilievo i principi della presunzione relativa di conformità, ai diritti fondamentali, dell'attività svolta dall'autorità giudiziaria estera nell'ambito di rapporti di collaborazione ai fini dell'acquisizione di prove, nonché dell'onere, in capo alla difesa, di allegare e provare il fatto dal quale dipende la violazione denunciata.

Il principio della presunzione di legittimità dell'attività compiuta all'estero ai fini dell'acquisizione di elementi istruttori, oltre ad essere oggetto di costante e generale enunciazione da parte della giurisprudenza di legittimità, trova una precisa base testuale nel Considerando (19) della Direttiva, secondo il quale «*la creazione di uno spazio di libertà, di sicurezza e di giustizia nell'Unione Europea si fonda sulla fiducia reciproca e su una presunzione di conformità, da parte di tutti gli Stati membri, al diritto dell'Unione e, in particolare, ai diritti fondamentali. Si tratta, però, di presunzione relativa. Di conseguenza, se sussistono seri motivi per ritenere che l'esecuzione di un atto di indagine richiesto in un OEI comporti la violazione di un diritto fondamentale e che lo Stato di esecuzione venga meno ai suoi obblighi in materia di protezione dei diritti fondamentali riconosciuti nella Carta, l'esecuzione dell'OEI dovrebbe essere rifiutata*».

Anche il principio in base al quale grava sulla difesa l'onere di allegare e provare il fatto dal quale dipende una causa di nullità o inutilizzabilità da essa eccepita è ripetutamente e generalmente ribadito dalla giurisprudenza di legittimità, rinvenendo, peraltro, ha una sua solida base normativa nell'art. 187 c.p.p., ai sensi del quale i fatti dai quali dipende l'applicazione di norme processuali sono oggetto di prova, non sussistendo, peraltro, dati normativi da cui inferire l'inversione, in questo specifico ambito, della regola generale secondo cui chi afferma l'esistenza di un fatto è gravato dell'onere della relativa prova.

Fermo tale principio, le Sezioni Unite hanno, dunque, condivisibilmente concluso che l'onere di allegare e provare i fatti da cui desumere la violazione di diritti fondamentali grava sulla difesa,

 Copyright © - www.quotidianolegale.it

quando è questa a lamentare l'inutilizzabilità o l'invalidità di atti istruttori acquisiti dall'autorità giudiziaria italiana mediante OEI.

Ovviamente, tale assetto normativo deve essere declinato in relazione allo specifico tipo di atto oggetto di richiesta e trasmissione.

Nel caso analizzato dal supremo Consesso, viene in rilievo l'acquisizione, da parte dell'autorità giudiziaria italiana, di comunicazioni scambiate su *chat* di gruppo mediante un sistema cifrato che era incontestabilmente già a disposizione dell'autorità giudiziaria francese.

Ne deriva che quanto chiesto dall'autorità giudiziaria italiana e consegnato dall'autorità giudiziaria francese, attiene a «*prove già in possesso delle autorità competenti dello Stato di esecuzione*» (per questa definizione le Sezioni Unite rimandano all'art. 1, par. 1, secondo periodo, della Direttiva 2014/41/UE, nonché, in termini analoghi, all'art. 2, comma 1, lett. a), d.lgs. n. 108/2017).

Ebbene, l'acquisizione di «*prove già in possesso delle autorità competenti dello Stato di esecuzione*» ha importanti conseguenze, in quanto è oggetto di alcune specifiche disposizioni derogatorie rispetto alla disciplina generale, funzionali a renderne più agevole la "circolazione".

Innanzitutto, osservano le Sezioni Unite, l'art. 10 Direttiva 2014/41/UE stabilisce che, nel caso di «*informazioni o prove che sono già in possesso dell'autorità di esecuzione quando, in base al diritto dello Stato di esecuzione, tali informazioni o prove avrebbero potuto essere acquisite nel quadro di un procedimento penale o ai fini dell'o.e.i.*», è esclusa la possibilità, per l'autorità di esecuzione, di disporre «*un atto di indagine alternativo*» a quello richiesto.

Inoltre, quando le prove richieste mediante OEI sono già in possesso dello Stato di esecuzione, la loro trasmissione allo Stato di emissione deve avvenire con immediatezza, perché non vi è alcun atto di indagine da compiere (artt. 12, par. 4, 13, par. 1, Direttiva 2014/41/UE).

Nella prospettiva interna, è risolutivo il rilievo che, nell'ordinamento giuridico italiano, la "circolazione" di prove già formate ha una disciplina specifica e diversa da quella riservata alla "formazione" di prove di identica tipologia.

Nel sistema processuale italiano, infatti, «*il pubblico ministero e, più in generale, la parte che vi ha interesse possono chiedere ed ottenere la disponibilità di prove già formate in un procedimento penale al fine di produrle in altro procedimento penale, senza necessità di alcuna autorizzazione preventiva da parte del giudice competente per quest'ultimo. Ciò anche nel caso di prove, come le intercettazioni di conversazioni o di comunicazioni, per la cui formazione è indispensabile la preventiva autorizzazione del giudice competente*».

 Copyright © - www.quotidianolegale.it

Numero 4 - 2024

Ovviamente, resta impregiudicato il potere del giudice competente per il procedimento penale nel quale le parti intendono avvalersi delle prove già separatamente formate o acquisite in altra sede di valutare se vi siano i presupposti per ammetterle ed utilizzarle ai fini della decisione.

Questo assetto normativo, affermano le Sezioni Unite, si ricava con chiarezza dagli artt. 238 e 270 c.p.p. e 78 disp. att. c.p.p. [12]

Gli atti oggetto dell'OEI costituenti «*prove già in possesso delle autorità competenti dello Stato di esecuzione*» possono essere, dunque, legittimamente richiesti e acquisiti dal pubblico ministero italiano, senza la necessità di preventiva autorizzazione del giudice del procedimento nel quale si "vorrebbe utilizzarli".

Unico presupposto di ammissibilità dell'ordine europeo di indagine, sotto il profilo del soggetto legittimato a presentarlo, è che, come detto, «*l'atto o gli atti di indagine richiesti nell'OEI avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo*».

Avuto, quindi, riguardo al regime interno della circolazione delle prove, quando l'OEI avanzato dal pubblico ministero italiano riguarda «*prove già in possesso delle autorità competenti dello Stato di esecuzione*», non vi sono ragioni per ritenere che il medesimo debba munirsi di preventiva autorizzazione del giudice del procedimento nel quale si vorrebbe utilizzare il materiale probatorio, siccome condizione non prevista nel nostro ordinamento, né altrimenti desumibile dal sistema dell'OEI, fermo restando, come dianzi chiarito, il potere del giudice di valutare se vi siano i presupposti per ammettere le prove ed utilizzarle ai fini delle decisioni di sua spettanza.

Il giudice, infatti, come già detto, può verificare se vi erano le condizioni per emettere l'OEI, così da assicurare il pertinente diritto di "impugnazione" nello Stato di emissione previsto dall'art. 14, par. 2, Direttiva 2014/41/UE, nonché se vi sia stata violazione dei diritti fondamentali riconosciuti dalla Costituzione e dalla Carta di Nizza, e, quindi, del diritto di difesa e della garanzia di un giusto processo, in linea con quanto stabilito dall'art. 14, par. 7, Direttiva 2014/41/UE.

Nell'incertezza, invece, del "tipo" di atto trasmesso (documenti informatici o dati concernenti il traffico, l'ubicazione e il contenuto di comunicazioni elettroniche) e della sua possibile qualificazione

[12] L'art. 238 c.p.p. detta le regole generali in tema di circolazione dei verbali di prove di altro procedimento e la disciplina, che riguarda anche gli atti irripetibili, non prevede, ai fini dell'acquisizione delle prove formate altrove, alcun intervento preventivo da parte del giudice del procedimento nel quale si chiede di utilizzarle. L'art. 270 c.p.p. indica i requisiti per la utilizzabilità dell'esito di attività di intercettazioni di conversazioni o comunicazioni disposte in altri procedimenti ed anche in questo caso, fermi i limiti, non è previsto alcun intervento preventivo del giudice del procedimento di destinazione. Infine, l'art. 78 disp. att. c.p.p. dispone che la documentazione di atti di un procedimento penale compiuti da autorità giudiziaria straniera può essere acquisita a norma dell'art. 238 c.p.p., con il solo ulteriore limite di cui al comma 2, a mente del quale, laddove si tratti di atto irripetibile, l'acquisizione al fascicolo del dibattimento è subordinata all'esame in contraddittorio o al consenso delle parti.

 Copyright © - www.quotidianolegale.it

come “risultato di intercettazioni”, le Sezioni Unite esaminano entrambe le prospettazioni, specificando anche che le stesse escludono esplicitamente che gli atti in questione costituiscano risultati di conversazioni o comunicazioni.

Nel primo caso (“documento informatico”), il parametro di riferimento interno, per verificare l’esistenza delle condizioni di ammissibilità dell’OEI e l’eventuale violazione di diritti fondamentali, è rappresentato dall’art. 234 c.p.p., a mente del è consentita l’acquisizione di scritti o di entità rappresentative di fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo, salvo che non contengano informazioni sulle voci correnti nel pubblico.

L’ampia latitudine operativa della norma, nella quale rientrano anche le comunicazioni elettroniche, risente, però, dell’applicazione, per alcune tipologie di documenti, di regole specifiche, in particolare nelle ipotesi in cui la prova documentale sia rappresentata da comunicazioni scambiate in modo riservato tra un numero determinato di persone, indipendentemente dal mezzo tecnico impiegato, a tal fine occorrendo assicurare la tutela prevista dall’art. 15 Cost. in materia di «corrispondenza».

Quello che rileva, infatti, è un concetto ampio che abbraccia ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza, che «prescinde dalle caratteristiche del mezzo tecnico utilizzato» e si estende, perciò, anche alla posta elettronica ed ai messaggi inviati tramite l’applicativo *WhatsApp*, o s.m.s., o comunque sistemi simili, «del tutto assimilabili a lettere o biglietti chiusi», in quanto accessibili solo mediante l’uso di codici di accesso o altri meccanismi di identificazione[13].

In tali casi, di conseguenza, occorre l’atto motivato dell’autorità giudiziaria con le garanzie stabilite dalla legge[14], non dovendo necessariamente tale atto promanare del “giudice”, essendo anche il pubblico ministero ricompreso nel sintagma «autorità giudiziaria», potendo egli, già per disposizioni codicistiche, sequestrare corrispondenza (art. 254 c.p.p.) e autorizzare l’acquisizione di plichi chiusi e di corrispondenza, anche in forma elettronica o inoltrata per via telematica (art. 353 c.p.p.), con il solo limite dell’acquisizione del documento presso lo studio del difensore[15].

Consegue che l’acquisizione di documenti, pur se relativi a “corrispondenza”, quando attiene a «*prove già in possesso delle autorità competenti dello Stato di esecuzione*», può essere chiesta

[13] Le Sezioni Unite citano, al riguardo, Corte cost., 27 luglio 2023, n. 170; nello stesso senso, Corte cost., 28 dicembre 2023, n. 227; Corte cost., 12 gennaio 2023, n. 2.
[14] Corte cost., n. 170/2023, cit.
[15] Per l’inclusione del pubblico ministero nella nozione di “autorità giudiziaria” anche nel diritto euro-unitario, le Sezioni Unite citano, proprio con riferimento alla Direttiva 2014/41/UE, la sentenza della CGUE, Grande Sezione, 8 dicembre 2020, Staatsanwaltschaft Wien, C-584/19.

 Copyright © - www.quotidianolegale.it

mediante OEI presentato dal pubblico ministero, senza necessità di autorizzazione del giudice, purché non si tratti di documentazione acquisita presso lo studio del difensore e con il divieto di acquisire corrispondenza tra imputato e difensore (divieto sancito dall'art. 103 c.p.p.).

Ovviamente, la qualificazione degli atti consegnati dall'autorità giudiziaria straniera in esecuzione di OEI in termini di documenti ha specifiche conseguenze con riguardo ai presupposti di ammissibilità della loro acquisizione e alla garanzia del rispetto dei «diritti fondamentali».

In tale prospettiva, allora, le Sezioni Unite, con riguardo al presupposto di ammissibilità di cui all'art. 6, paragrafo 1, lett. b), Direttiva 2014/41/UE, relativo alla c.d. valutazione in astratto, affermano che è sufficiente considerare che anche l'acquisizione "originaria" della prova documentale, nel sistema processuale italiano, pur quando abbia ad oggetto "corrispondenza", può essere disposta dal pubblico ministero, con atto motivato, senza alcuna autorizzazione del giudice, salvo, come detto, il caso di sequestro effettuato nell'ufficio di un difensore.

Di conseguenza, se l'ordine europeo di indagine presentato dal pubblico ministero ha ad oggetto l'acquisizione di documenti e "corrispondenza" non costituenti «*prove già in possesso delle autorità competenti dello Stato di esecuzione*», il rispetto della condizione che esige il potere dell'autorità di emissione di disporre «*l'atto o gli atti di indagine richiesti nell'OEI [...] alle stesse condizioni in un caso interno analogo*» è assicurato anche in assenza di una autorizzazione del giudice, salvi i divieti di cui all'art. 103 c.p.p.

A maggior ragione, quindi, l'acquisizione di documenti, pur se relativi a "corrispondenza", qualora attenga a «*prove già in possesso delle autorità competenti dello Stato di esecuzione*», può essere chiesta mediante OEI presentato dal pubblico ministero, senza necessità di autorizzazione del giudice.

Per quanto riguarda il rispetto dei «diritti fondamentali», poi, la qualificazione degli atti consegnati dall'autorità giudiziaria straniera in esecuzione di OEI come documenti, specie se costituiscono "corrispondenza", comporta, soggiungono le Sezioni Unite, l'esigenza di specifica attenzione a profili contenutistici degli stessi. Ad esempio, un principio generale in materia di tutela di diritto di difesa, positivizzato nel sistema italiano dall'art. 103 c.p.p., è, come in precedenza anticipato, quello del divieto di sequestro e di ogni forma di controllo della «corrispondenza» tra l'imputato ed il suo difensore, salvo il fondato motivo che si tratti di corpo del reato. Resta fermo, ribadisce la Corte, che l'onere dell'allegazione e della prova in ordine ai fatti da cui desumere la violazione dei «diritti fondamentali» grava sulla parte interessata.

Quanto, invece, alla qualificazione alternativa dell'atto come «dati concernenti il traffico, l'ubicazione, e il contenuto di comunicazioni elettroniche», di cui si è dato conto, oggetto anch'essa di analisi da parte delle Sezioni Unite, la stessa comporta che la loro acquisizione sia soggetta alla

 Copyright © - www.quotidianolegale.it

disciplina interna, la quale richiede, come presupposti indefettibili, sia la necessità degli stessi ai fini dello svolgimento di indagini per un reato «grave», sia la preventiva autorizzazione del giudice.

In forza della disciplina italiana (cfr. art. 132 d.lgs. n. 196/2003, 30 giugno 2003, n. 196, modificato, come detto, dall'art. 1, comma 1, d.l. n. 132/2021, convertito, con modificazioni, dalla l. n. 178/2021), allora, i dati relativi al traffico telefonico o telematico possono essere acquisiti presso il fornitore, solo se:

a) sussistano sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, o di altri reati specificamente indicati;

b) detti dati siano «rilevanti per l'accertamento dei fatti»;

c) vi sia stata precedente autorizzazione rilasciata dal giudice con decreto motivato, ovvero il provvedimento del pubblico ministero adottato in caso di qualificata urgenza, sia stato convalidato con decreto motivato del giudice entro il termine massimo di novantasei ore.

Occorre a tal proposito osservare che la disciplina dettata dall'art. 132 d.lgs. n. 196/2003 non è derogata da quella prevista dall'art. 45 d.lgs. n. 108/2017, ai sensi del quale l'OEI «*al fine di ottenere i dati esterni relativi al traffico telefonico o telematico nonché l'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni*» possa essere presentato sia dal giudice, sia dal pubblico ministero. Al riguardo, infatti, come correttamente evidenziano le Sezioni Unite, «*ritenere che il pubblico ministero abbia l'obbligo di ottenere la preventiva autorizzazione del giudice del procedimento nel quale intende utilizzare dati relativi al traffico telefonico o telematico, quando occorre richiederli ad un gestore operante in Italia, e non anche quando sia necessario richiederli ad un gestore estero, sarebbe in contrasto con la prescrizione dell'art. 6, par. 1, lett. b), Direttiva 2014/41/UE, la quale esige che l'autorità di emissione abbia il potere di disporre l'atto o gli atti di indagine richiesti nell'OEI [...] alle stesse condizioni in un caso interno analogo*».

La disciplina che richiede la preventiva autorizzazione del giudice, tuttavia, si riferisce all'acquisizione dei dati presso il gestore dei servizi telefonici e telematici, ma non involge la loro utilizzazione in un procedimento penale diverso da quello in cui sono stati già acquisiti.

L'art. 132 d.lgs. n. 196/2003, infatti, fa riferimento ai dati relativi al traffico telefonico e al traffico telematico «conservati dal fornitore» (così testualmente il comma 1).

Tale interpretazione, soggiunge il supremo Consesso, non si pone in contrasto con il diritto euro-unitario avendo la Corte di giustizia statuito che «*l'art. 15, par. 1, della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, letto alla luce degli articoli 7, 8 e 11, nonché dell'art. 52, par. 1, della Carta dei diritti fondamentali, osta ad una normativa nazionale che renda*

 Copyright © - www.quotidianolegale.it

il pubblico ministero 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»[16].

Nelle ipotesi in cui, però, detti elementi siano già stati acquisiti in un procedimento penale, non si è più al cospetto di un'autorizzazione all'accesso di un'autorità pubblica, nella misura in cui gli stessi sono già a disposizione di una pubblica autorità.

In conclusione: nel sistema processuale italiano, il pubblico ministero può acquisire presso altra autorità giudiziaria dati relativi al traffico o all'ubicazione, concernenti comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica, senza dover chiedere preventiva autorizzazione al giudice competente per il procedimento nel quale intende utilizzarli.

Di conseguenza, deve, allora, ritenersi che un OEI formulato dal pubblico ministero italiano con il quale si richiede, senza preventiva autorizzazione del giudice nazionale, la trasmissione di dati della medesima tipologia, già acquisiti dall'autorità giudiziaria straniera in un procedimento penale pendente innanzi ad essa, abbia ad oggetto atti che «*avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo*».

Quanto, invece, al tema riguardante la garanzia del rispetto dei «diritti fondamentali», le Sezioni Unite, come rilevato, osservano che, anche in ragione della specifica elaborazione della giurisprudenza della Corte di giustizia[17], «*l'originaria acquisizione presso il gestore dei servizi telefonici e telematici dei dati relativi al traffico o all'ubicazione, concernenti comunicazioni elettroniche, deve essere stata preventivamente autorizzata da un giudice o da un'autorità amministrativa indipendente, non coinvolta nelle indagini e in posizione di terzietà rispetto all'esito del procedimento*».

In tale ottica, allora, giova ribadire che non viola i «diritti fondamentali» l'acquisizione dei predetti dati da parte del pubblico ministero, senza preventiva autorizzazione del giudice competente per il procedimento nel quale si intende utilizzarli, quando gli stessi siano già stati acquisiti, previa autorizzazione del giudice competente, in altro procedimento.

Analoghe considerazioni, in punto di insussistenza di violazione dei diritti fondamentali, debbono essere spese con riferimento all'accesso ad un'ampia mole di dati relativi al traffico e all'ubicazione, concernenti comunicazioni elettroniche. Rimarcano, su tale aspetto, le Sezioni Unite con le sentenza in commento che la giurisprudenza della Corte di giustizia non pone, invero, alcun limite quantitativo,

[16] CGUE, Grande Sezione, 2 marzo 2021, H.K./Prokuratuur, C-746/18.
[17] CGUE, Grande Sezione, 2 marzo 2021, H.K./Prokuratuur, cit.; cfr., nello stesso senso, CGUE, Grande Sezione 5 aprile 2022, Commissioner of An Garda Sfochana, C-140/20, §§ 107, 108, 109 e 110; CGUE, Quarta Sezione, 16 dicembre 2021, HP, C-724/19, § 42.

 Copyright © - www.quotidianolegale.it

richiedendo, invece, «*criteri oggettivi per definire le circostanze e le condizioni in presenza delle quali deve essere concesso alle autorità nazionali competenti l'accesso ai dati in questione*», indicando, come accessibili, «*i dati di persone sospettate di progettare, di commettere o di aver commesso un illecito grave, o anche di essere implicate in una maniera o in un'altra in un illecito del genere*»[18] .

Il supremo Consesso esclude, inoltre, che «*l'impossibilità, per la difesa, di accedere all'algoritmo utilizzato*» - aspetto sul quale in tutti procedimenti in corso si è ampiamente discusso e dibattuto - «*nell'ambito di un sistema di comunicazioni per "criptare" il contenuto delle stesse*» dia luogo ad una violazione di diritti fondamentali.

A tal riguardo le Sezioni Unite osservano, infatti, che sebbene la disponibilità dell'algoritmo di criptazione sia funzionale ad un accertamento circa l'affidabilità del contenuto delle comunicazioni acquisite al procedimento, tuttavia «*il pericolo di alterazione dei dati non sussiste, salvo specifiche allegazioni di segno contrario, in quanto il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, per cui una chiave errata non ha alcuna possibilità di decriptarlo, anche solo parzialmente*».

D'altra parte, la giurisprudenza sovranazionale – come segnalato sul punto dalla Cassazione nelle sentenze in disamina – parrebbe non aver mai affermato che l'indisponibilità dell'algoritmo di decriptazione agli atti del processo costituisca, di per sé, violazione dei diritti fondamentali; anzi, con la sentenza 26 settembre 2023, Y.Y. c. Turchia, § 336, la Corte EDU, Grande Camera, pronunciandosi in relazione ad una vicenda in cui i dati acquisiti non erano stati messi a disposizione della difesa e la pronuncia di colpevolezza si era fondata sul mero (e solo) uso di un sistema di messaggistica criptata denominato *Bylock*, si è limitata ad affermare che attribuire al ricorrente l'opportunità di prendere conoscenza del materiale decriptato avrebbe potuto costituire un passo importante per preservare i suoi diritti di difesa senza, al contempo, affermare che tale mancata messa a disposizione integrasse un *vulnus* dei diritti fondamentali.

Resta fermo, ancora una volta, che l'onere dell'allegazione e della prova in ordine ai fatti da cui desumere la violazione dei «diritti fondamentali» grava sulla parte interessata e, *a contrariis*, anche il solo utilizzo di criptofonini, mezzo ritenuto inattaccabile a tutela di comunicazioni illecite, è divenuto, grazie ai profusi sforzi delle forze dell'ordine, un possibile elemento a carico.

[18] CGUE, Grande Sezione, 2/3/2021, H.K./Prokuratuur, cit., § 50; CGUE, Grande Sezione, 5 aprile 2022, Commissioner of An Garda Sfochana, cit., § 105.

 Copyright © - www.quotidianolegale.it

Di qui l'affermazione dei principi di diritto sopra indicati, in attuazione dei quali le Sezioni Unite hanno rigettato i ricorsi.

5. Riflessioni finali.

Le Sezioni Unite, come esposto, hanno aderito, tra quelle in premessa indicate, alla terza scuola di pensiero, secondo la quale la richiesta da parte dell'autorità giudiziaria italiana, mediante ordine europeo di indagine, volto ad acquisire comunicazioni scambiate in *chat* di gruppo con sistema cifrato, già ottenute e decifrate dall'autorità giudiziaria estera, è regolata dalla disciplina generale relativa alla circolazione delle prove tra procedimenti penali, come desumibile dal codice di rito.

Il riferimento è alle disposizioni di cui agli artt. 238 e 270 c.p.p. e 78 disp. att. c.p.p., le quali consentono al pubblico ministero di disporre l'acquisizione di dati o prove acquisite in un diverso procedimento penale.

Tale soluzione è perfettamente compatibile con l'insegnamento della Corte costituzionale sulla tutela della corrispondenza – essendo rispettata, con il provvedimento del pubblico ministero di acquisizione, la riserva di legge prevista dall'art. 15 Cost., non ponendosi, neppure, in contrasto con la disciplina dettata dall'art. 132 del d.lgs. n. 196/2003 per l'acquisizione di dati relativi al traffico telefonico e telematico – che richiede la preventiva autorizzazione del giudice – giacché tale normativa attiene ai dati da acquisire presso i relativi gestori e non quelli già acquisiti dall'autorità giudiziaria estera.

In ogni caso, resta salvo il potere del giudice italiano di valutare l'utilizzabilità ai fini della decisione di tali elementi, la quale andrà esclusa soltanto qualora la stessa comporti una violazione dei diritti fondamentali, che deve essere allegata e provata dalla parte che l'ha eccepita.

Il giudice nomofilattico, pertanto, fornisce una soluzione che risponde, in primo luogo, all'esigenza di rapida acquisizione dei dati necessari ai fini di indagine – attribuendo il relativo potere al pubblico ministero senza necessità della preventiva autorizzazione giudiziale – al contempo assicura la tutela dei diritti dei soggetti coinvolti attraverso il controllo successivo del giudice, il quale, come detto, dovrà escludere l'utilizzabilità dei dati acquisiti se la parte che eccepisce la relativa invalidità adempie all'onere di allegazione e di dimostrazione, in termini concreti, della lesione dei suoi diritti fondamentali previsti dalla Costituzione e dalla Carta di Nizza, in particolare, del diritto di difesa e del diritto al giusto processo.

 Copyright © - www.quotidianolegale.it

Inoltre, aderendo sul punto alla tesi più risalente, la Corte supera anche l'eccezione relativa all'impossibilità per la difesa di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per criptare il testo delle stesse, chiarendo che tale circostanza non determina una violazione dei diritti fondamentali, giacché, salvo specifiche allegazioni di segno contrario, non ricorre il pericolo di alterazione dei dati, in considerazione del fatto che il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, ragione per cui una chiave errata non ha alcuna possibilità, neppure parziale, di decriptazione.

Le Sezioni Unite, dunque, nel dirimere i contrasti interpretativi, realizzano l'equo contemperamento tra la necessità di acquisire velocemente gli elementi investigativi – attribuendo il relativo potere direttamente al pubblico ministero, così tutelando anche la riserva di giurisdizione prevista dall'art. 15 Cost., nel caso in cui i dati conservati all'estero costituiscano corrispondenza, nell'accezione fornita dalla Corte costituzionale – e quella di garantire, comunque, il controllo sul rispetto dei diritti fondamentali della persona, attraverso l'intervento successivo del giudice italiano, chiamato a vagliare l'eventuale inutilizzabilità dei dati richiesti e ottenuti dall'autorità giudiziaria estera, nel caso in cui la loro utilizzazione si ponga in contrasto con i diritti fondamentali della persona, a condizione che il soggetto che la eccepisce dimostri rigorosamente, giova ribadire, la lesione delle sue garanzie costituzionalmente e convenzionalmente previste[19].

[19] S. PIGNATA, *Le Sezioni unite sull'utilizzabilità della messaggistica criptata acquisita mediante ordine europeo di indagine,* in *www.penaledp.it*, 1 luglio 2024.

 Copyright © - www.quotidianolegale.it