GIURISPRUDENZA PENALE

I limiti di utilizzabilità della messaggistica criptata SkyEcc acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali.

di ***Matteo Rampioni***

Sommario. 1. Premessa. – **2.** I sistemi di comunicazione crittografati. – **3.** La natura ed il regime di utilizzabilità della messaggistica criptata Sky-Ecc. – **4.** Riflessioni. **A)** La natura giuridica dei dati acquisiti. – **B)** L'incompatibilità con le indicazioni provenienti dalla Corte di Giustizia Europea. – **C)** SkyEcc e principio del contraddittorio.

1. Premessa.

Gli strumenti di cooperazione giudiziaria internazionale rivestono un ruolo sempre più determinante nella battaglia al crimine internazionale.

Negli ultimi anni, attraverso la creazione di apposite "task force operative" europee, le diverse Autorità giudiziarie hanno avuto modo di accertare come determinate attività illecite (in particolare quelle legate al traffico di stupefacenti) vengono oramai condotte e realizzate a distanza mediante l'utilizzo di telefonia criptata.

Nel tentativo di arginare simili condotte criminali le interforze europee coordinano una serie di indagini funzionali ad acquisire e decriptare le comunicazioni (chat) generate e scambiate da migliaia di utenti in tutto il mondo.

Con una prima operazione, denominata "Emma95" (del mese di giugno 2020), la polizia olandese, la gendarmeria francese e le rispettive Autorità giudiziarie, mettono sotto "assedio" il sistema crittografato "Enchrochat".

Una volta individuati i server (situati in Francia), si istituisce una task-force operativa (OTF) presso Europol per consentire: dapprima l'hackeraggio dei terminali in questione; poi la condivisione dei dati acquisiti con i paesi maggiormente interessati (tra cui anche l'Italia) dall'uso illegale di questi telefoni.

Sulla base di tali dati, nel marzo 2020, 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.

Nel mese di marzo 2021, sempre le Autorità francesi, belghe e olandesi, nell'ambito di una "Joint Investigation Team", sviluppano un'indagine

internazionale su larga scala denominata "Argus". Questa volta la piattaforma criptata d'interesse è quella denominata "Sky Ecc".
Anche in questo caso, dopo aver violato i server (sempre allocati in Francia), si acquisiscono e decriptano centinaia di milioni di messaggi scambiati tra i diversi utenti in tutto il mondo da cui scaturiscono, anche in questo caso, numerosi arresti e sequestri (di droga, armi e denaro).
Gli Uffici di Procura italiani entrano in possesso della messaggistica (già) decriptata 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[1].
L'acquisizione della messaggistica da 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.
La materia oggetto di trattazione, quantomeno nella prospettazione di chi scrive, presenta diversi profili d'interesse: innanzitutto, poiché il tema delle conversazioni criptate viene affrontato sotto una diversa angolazione rispetto a quanto sino ad oggi fatto[2]; poi, perché evidenzia come i tradizionali

[1] Cass., sez. IV, 12 aprile 2023, n. 18523, in *www.dejure.it*. «Il Tribunale ha chiarito che il sistema Sky Ecc consente lo scambio di comunicazioni mediante uso di cripto-telefonini o smartphones, modificati in modo da garantire la inviolabilità. La violazione della piattaforma criptata era avvenuta da parte di law enforcement agencies e il suo utilizzo si era arrestato nel marzo del 2021, allorquando si era diffusa la notizia dell'avvenuta violazione. Gli esiti dell'indagine presupposta avevano consentito di acquisire e analizzare milioni di messaggi scambiati tra membri di organizzazioni criminali operanti in vari Paesi UE ed è in questo contesto si era inserita l'indagine condotta dalla Procura di Reggio Calabria. La Polizia giudiziaria, infatti, analizzando il traffico telefonico storico delle celle abitualmente abbinate ad utenze ufficiali in uso agli indagati, aveva individuato alcuni pin collegati alla piattaforma criptata. Conseguentemente il Pubblico Ministero procedente aveva tramite O.E.I. rivolti all'Autorità giudiziaria francese richiesto le trasmissioni dei messaggi già decifrati riferibili alle comunicazioni che avevano riguardato i PIN d'interesse, conservate in un server».

[2] Sino ad oggi, infatti, la questione che gravitava attorno alle conversazioni cifrate (le comunicazioni con telefoni Blackberry) era quella relativa alla necessità o meno della rogatoria internazionale allorquando per la decriptazione si rendeva necessaria la collaborazione del produttore del sistema operativo.
Sul punto la Cassazione stabiliva che l'attività di intercettazioni delle comunicazioni intercorse attraverso telefoni Blackberry, non richiedesse alcuna rogatoria internazionale (verso il Canada dove fisicamente è presente il server della società che utilizza il sistema cosiddetto "pin to pin"). Si tratterebbe, infatti, di captazione in tempo reale anche se il segnale viaggia prima criptato e viene poi reso intellegibile dalla trasformazione operata dal server cui si affida la società Blackberry.

sistemi investigativi non sono più sufficientemente efficaci per contrastare talune fattispecie di reati[3], evidenziando al contempo, da un lato l'evoluzione tecnologica per la commissione di illeciti (in particolare quelli legati al commercio di sostanza stupefacente e quelli previsti in materia di associazione per delinquere di stampo mafioso)[4], dall'altro una necessaria, e sempre maggiore, cooperazione tra le diverse autorità giudiziarie; infine, perché, alla luce della recente giurisprudenza che si sta formando in materia, apre la strada ad una serie di questioni interpretative (tra cui la corretta qualificazione giuridica del materiale probatorio acquisito tramite O.I.E, il suo regime di utilizzabilità (anche alla luce dei principi sanciti dalla Corte di Giustizia europea) e, in conclusione, il tema relativo al rispetto del principio del contraddittorio anche nella fase acquisitiva delle fonti di prova[5].

2. I sistemi di comunicazione crittografati.

Ai fini della presente ricerca può essere utile, seppur brevemente, comprendere il funzionamento dei sistemi crittografati.

Non scatta quindi alcuna rilevanza extraterritoriale della captazione che obblighi il giudice a richiedere l'attività di cooperazione giudiziaria al proprio omologo straniero.
Tra le varie: Cass. sez. VI, 20 aprile 2021, n.18907, in *www.dejure.it*; Cass., sez. IV, 26 ottobre 2022, n. 49411, in *www.dejure.it*; Cass., sez. VI, 18 gennaio 2023, n. 8714 in *www.dejure.it*.

[3] L. Palmieri, *La nuova disciplina del captatore informatica tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza "Scurato" alla riforma sulle intercettazion*i, in *Dir. pen. con*t., 1/2018, p. 59 «Il nuovo volto della criminalità ha posto i sistemi di indagine tradizionali in grave difficoltà, evidenziando l'incapacità investigativa delle Autorità Giudiziaria di contrastare, in maniera efficace, il traffico di droga e la cessione di materiale pedopornografico. Solo con il ricorso alle indagini informatiche gli organi investigativi sono posti in condizione di ricercare ed assicurare il dato probatorio».

[4] F.R. Dinacci, *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, Milano, 2008, p. 141 «L'evoluzione di spazi giuridici sovranazionali e la loro regolamentazione in continuo divenire suggerisce di valutare il perimetro operativo dell'inutilizzabilità anche con riferimento alla prova assunta all'estero. L'attualità del tema non deriva solo dalla constatazione di un incremento del cd. crimine transfrontaliero, ma anche dalla continua evoluzione degli strumenti tecnologici. Gli stessi, infatti, sono di tale natura che rendono possibile realizzare la condotta in un determinato luogo con verificazione degli effetti in sede distinta. […]. Ancora una volta l'evoluzione tecnologica pone la scienza giuridica in una posizione di perenne "affanno" determinato dall'impossibilità di adeguarsi ed evolversi ala stessa velocità delle innovazioni tecnologiche; queste ultime, peraltro, risultano foriere di nuovi scenari giuridici a cui non sempre gli instrumencta dell'ordinamento risultano in grado di soccorrere allo scopo».

[5] Cass., sez. IV, 15 luglio 2022, n. 32915, in *Guida al diritto*, 2022, p. 38.

Nel 1990 la Telecom Italia converte le proprie centrali analogiche elettromeccaniche in centrali a tecnologia digitale, implementando la tecnologia *ISDN* (Integrated Services Digital Network) grazie alla quale divengono supportati i servizi portanti, i tele-servizi, ed i servizi c.d. supplementari (quali, ad esempio, l'identità del chiamante, il trasferimento di chiamata).
Nel medesimo periodo la Telecom Italia da avvio al proprio sistema di chiamate in mobilità denominato *E-Tacs* che sostituisce il precedente *RTMI*.
Nel 1995 in Italia diventa pienamente operativa la prima rete di comunicazioni radiomobili in tecnologia *GSM* (cd. tecnologia di generazione 2G) mediante cui si apportano numerose innovazioni, tra le quali: la completa cifratura delle trasmissioni che impedisce intercettazioni illegali; una miglior efficienza spettrale che consente di usufruire di "servizi dati" come l'invio e la ricezione di messaggi di testo (Sms)[6].
La rete *GSM* viene successivamente implementata dalle tecnologie *GPRS* ed *EDGE* (convenzionalmente definite di generazione *2.5G*) grazie alle quali gli utenti possono usufruire, nell'ambito dei sistemi di messaggistica testuale di funzionalità per l'invio e la ricezione di file multimediali (video e messaggi vocali).
Con l'ulteriore sviluppo delle reti radiomobili (tecnologia *UMTS,* altrimenti chiamata *3G*) si può iniziare ad usufruire anche della videochiamata, della videoconferenza e della connessione alla rete internet che consente la navigazione sul Web[7].
Le successive tecnologie standard *LTE* e *5G* ampliano ulteriormente le capacità comunicative in termini di velocità di trasmissione e ricezione dati[8].
L'evoluzione dei sistemi di telecomunicazione favorisce lo sviluppo di molteplici tecnologie tra le quali, una delle più rilevanti, è costituita dalla possibilità di effettuare chiamate ed inviare messaggi sfruttando semplicemente la rete internet ed i suoi protocolli di trasmissione (la tecnologia *VoIP*[9]).
Lo sviluppo e l'implementazione della tecnologia *VoIP* da il via alla diffusione di numerosissime applicazioni quali *Skype, WhatsApp, Signal, WikrMe, Zfone, PrivateWave*, utilizzabili sia mediante personal computer che tramite

[6] M. Redl, M.K. Weber, M.W. Oliphant, *An Introduction to GSM. In Artech House, 1995, p. 1 ss; M. Sauter, From GSM to LTE-Advanced Pro and 5G: An introduction to mobile Networksand and mobile Broadband*, Wiley, IV ed., 2021, p. 1 ss.
[7] F. Muratore, *Le comunicazioni mobili del futuro, UMTS: il nuovo sistema del 2001*, CSELT, 2000; R. Kreher – T. Ruedebusch, *UMTS Signaling: UMTS Interfaces, Protocols, Message Flows and Procedures Analyzed an Explai*ned, Wiley, 2005, p. 1 ss.
[8] M. Sauter, *From GSM to LTE-Advanced Pro and 5G: An introduction to mobile Networksand and mobile Broadband*, op. cit., p. 1 ss; C. Cox, *An Introduction to LTE, LTE-Advanced, SAE, VoLTE and 4G Mobile Communications*, Wiley, II ed., 2014, p. 1 ss.
[9] J.M. Huerta – R. M. Stern, *Speech recognition from GSM codec parameters*, in *cs.cmu.edu*, 23 giugno 2015.

smartphone, per la realizzazione di comunicazioni in fonia, video-conference, senza limitazioni geografiche e senza costi.
Tutte queste applicazioni si basano sull'utilizzo del protocollo *TCP-IP* che consente l'invio e la ricezione dei dati (incapsulati in "pacchetti") tra due terminali, sfruttando un protocollo denominato *HTTP* (Hypertext Transfer Protocol)[10].
La trasmissione dei dati avviene in maniera non crittografata e, dunque, consente l'eventuale intercettazione dei pacchetti trasmessi e ricevuti.
Al fine di ovviare a tale problematica la Netscape Communication Corporation progetta ed integra il protocollo *HTTPS*[2] [11]che fornisce una cifratura bidirezionale delle comunicazioni, garantendo così che i contenuti delle comunicazioni non possano essere intercettati o alterati da terzi[12].
L'unico modo per captare i messaggi e le comunicazioni "coperte" da cifratura è l'installazione di un *malware* sul telefono oggetto di interesse.
In questo modo «l'agente intrusore» riesce ad operare in modalità "*fully-aquiring*", by-passando i sistemi di garanzia e consentendo di leggere direttamente quanto appare sul display prima che i dati vengano criptati.
Proprio per questo, alcune aziende specializzate del settore sviluppano soluzioni *stand-alone* (*Encrochat, Kline Plus*) che prevedono l'implementazione di un'applicazione di messaggistica istantanea e/o di funzioni di chiamate su smartphone appositamente modificati nell'hardware e nel software che rende meno agevole l'inoculazione del captatore informatico.
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 è protocollo che consente di effettuare chiamate criptate su rete internet).
Utilizza questa tecnologia, il sistema *SkyEcc*.
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

---

[10] E.Gregersen, *Voce Hyperttext Transfer Protocol*, in *Encyclopaedia Britannica*, www.britannica.com; M. Bossi, *Definizione e significato di http, in www.mrv.it*, 8 marzo 2017.
[11] M. Thomson (ed.), M. Belshe e R. Peon, *Hypertext Transfer Protocol version 2 - draft-ietf-httpbis-http2-16, su ietf.org, HTTPbis Working Group; R. Brian, Wait for it – HTTP/2 begins Working Group Last Call!*, in *www.msopentech.com*, Microsoft Open Technologies, 7 agosto 2014; S. Anthony, S&M vs. SPDY: Microsoft and Google battle over the future of HTTP 2.0, in www.extremetech.com, 28 marzo 2012.
[12] F. Carli, *La crittografia: cos'è, come funziona e perché è alleata della sicurezza informatica*, in *Network Digital 360*, 21 ottobre 2022.

dispositivo verifica la sicurezza della connessione al Server (se vengono riscontrati problemi di sicurezza non è possibile utilizzare il sistema di messaggistica *SkyEcc*); 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 *SkyEcc* prevede, inoltre, ulteriori forme di «protezione»: quella della cancellazione automatica dei messaggi dopo trenta secondi; quella della 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[13]; le SIM utilizzate sui propri dispositivi sono registrate e di sua proprietà, non consentendo così di risalire all'utente; nessun messaggio sarà mai, ed in ogni caso, conservato sul server per più di quarantotto ore.

3. La natura ed il regime di utilizzabilità della messaggistica criptata Sky-Ecc.

Secondo l'orientamento (di legittimità e di merito) che si sta consolidando in materia[14], i dati trasmessi dalle Autorità francesi alle diverse Procure italiane tramite Ordine Europeo di Indagine andrebbero considerati documenti informatici ai sensi dell'art. 234-*bis* c.p.p[15].
Le ragioni sarebbero molteplici.
Innanzitutto, si tratterebbe di contenuti di conversazioni testuali o di messaggistica vocale riversati dall'Autorità francese all'interno di supporti informatici (CD-ROM).
Non si verterebbe, dunque, nell'ambito delle intercettazioni telefoniche o telematiche che, come è noto, trovano un'autonoma disciplina ai sensi degli artt. 266 e ss. c.p.p.[16], in quanto difetterebbero tutti e due gli elementi

[13] Da fonte aperta *https://web.archive.org/web/20191108032430/https://www.skyglobal.com/products/*.
[14] Cass., sez. VI, 27 aprile 2020, n. 12975, in www.dejure.it; Cass., sez. IV, 4 aprile 2023, n. 18511, in www.dejure.it; Cass., sez. IV, 12 aprile 2023, n. 18523, in www.dejure.it; Cass., sez. IV, 18 aprile 2023, n. 16347, in www.dejure.it; Tribunale di Reggio Calabria, Sezione per il Riesame delle misure cautelari personali, Ord. 5 novembre 2022, n. 801; Tribunale di Reggio Calabria, Sezione per il Riesame delle misure cautelari personali, Ord. 19 novembre 2022, n. 868.
[15] Art. 234-bis c.p.p. «E' 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».
[16] Per una panoramica sulla prova documentale: L. Maggio, voce *Prova documentale*, in *Enc. Giur*., XXV, Roma, 1991, p. 1; R. D'Isa, *Sulla disciplina dei documenti nel processo penale*, in *Riv. It. Dir. Pen. Proc*., 1992, p. 1412; P. Calamandrei, *I documenti in senso stretto nell'ottica del codice del 1988*, in *Giust. pen*., 1992, III, p. 76; P. Calamandrei, *La*

necessari per applicare la (più garantita) disciplina delle intercettazioni telefoniche o telematiche: da un lato, il cd. «flusso di comunicazioni»; dall'altro, la cd. «apprensione occulta»[17].

Non mancherebbe poi, secondo l'indirizzo in questione, neppure il requisito del «consenso del legittimo titolare» (richiesto dall'art. 234-*bis* c.p.p.) per l'acquisizione di quei dati conservati in Francia, dovendosi intendere con tale locuzione la persona (fisica o giuridica) che di quei documenti può giuridicamente disporre, in forza di un legittimo titolo, secondo le norme dell'ordinamento giuridico del paese estero (identificabile nella specie con l'autorità giudiziaria francese che legittimamente ha acquisito i dati e li detiene[18]).

A tal proposito la Suprema Corte[19] stabilisce che, ai fini dell'applicazione dell'art. 234-*bis* c.p.p., è documento informatico ogni rappresentazione comunicativa incorporata su di una base materiale con un metodo digitale ed è il legittimo titolare la persona giuridica che può legittimamente disporre del documento.

Ne consegue che, se l'autorità giudiziaria di uno Stato dell'Unione Europea, in attuazione della Direttiva 2014/41/UE, dà esecuzione a un O.I.E. emesso dall'Autorità giudiziaria di altro Stato membro, trasmettendo dati che ha ottenuto in conformità alla propria legislazione interna ed ha incorporato in una base comunicativa con metodo digitale (come quelli di cui si sta

---

prova documentale, Padova, 1995, p. 1 ss.; P. Calamandrei, *Premesse definitorie e classificazioni in tema di prova documentale*, in *Dig. Pen*., X, Torino, 1995, p. 384; R. Cantone, *La prova documentale*, Milano, 2004, p. 1 ss.; S. Aterno, *L'acquisizione di dati personali tra misure antiterrorismo e intromissione nella privacy*, in *Arch. pen*., 2016, p. 165.

[17] Cass., sez. IV, 12 aprile 2023, n. 18523, in *www.dejure.it* «Il pubblico ministero, con gli O.E.I. in esame, ha chiesto la trasmissione di documentazione già acquisita dall'autorità estera nel corso di un diverso procedimento penale in quel Paese. L'ordine europeo di indagine doveva solo dar conto dello specifico oggetto della prova, essendo rimessa allo Stato di esecuzione, con le modalità previste in quell'ordinamento, la concreta acquisizione della prova, da trasferire poi allo Stato di emissione: nella specie, come detto, la richiesta ha riguardato le chat del sistema Sky Ecc., già acquisite dal Tribunal judiciarie de Paris autonomamente e non su richiesta della Procura procedente nel nostro Paese. L'autorità francese, dunque, si è resa garante, in assenza di specifiche deduzioni di segno diverso, del rispetto delle procedure dello Stato di esecuzione (la Francia), avendo il Tribunale del riesame dato atto che dalla documentazione trasmessa era dato verificare le modalità di acquisizione e conservazione dei dati da parte dell'Autorità giudiziaria francese. La messaggistica esaminata dal Tribunale di Reggio Calabria non costituisce esito di captazione di conversazione durante il flusso dinamico delle stesse, bensì acquisizione di dati informatici direttamente utilizzabili ai fini di prova».

[18] Tribunale di Reggio Calabria, Sezione per il Riesame delle misure cautelari personali, Ord. 5 novembre 2022, n. 801.

[19] Cass., sez. I, 1 luglio 2022, n. 34059, in *www.dejure.it*.

discutendo[20]), vi sarà sempre il consenso del legittimo titolare richiesto dall'art. 234-*bis* c.p.p.
A conferma della natura documentale della messaggistica rileverebbe poi, sempre secondo l'indirizzo in questione, il fatto che l'Autorità giudiziaria italiana, secondo i principi vigenti in materia di cooperazione internazionale, non ha inteso partecipare in alcun modo alle diverse fasi di formazione della prova.
A tal proposito, l'impostazione esegetica in commento ricorda come in materia di Ordine d'indagine europeo vige il principio di diritto, già espresso in tema di rogatoria internazionale, secondo cui trovano applicazione, da un lato il principio "*locus regit actum*"; dall'altro, in conformità ai canoni di diritto internazionale, quello della prevalenza della "*lex loci*" sulla "*lex fori*".
La *ratio* di tale assunto, così come osserva la Suprema Corte di Cassazione[21], sarebbe coerente con la più recente evoluzione del panorama normativo internazionale e comunitario tesa a rendere, non solo, più snella ed efficace la mutua assistenza giudiziaria; ma, soprattutto, funzionale e diretta a superare il concetto di "assistenza" per sostituirvi quello di "cooperazione", ritenuta necessaria per una più efficace lotta contro il crimine transnazionale. Tutto ciò sul presupposto: da un lato, della sostanziale conformità degli ordinamenti degli Stati europei agli stessi fondamentali principi di tutela dei diritti fondamentali della persona; dall'altro, sulla base della mutua fiducia nella capacità degli Stati stessi di garantire un equo processo.
In linea con tale richiamo si stabilisce[22] che l'utilizzazione degli atti trasmessi da Autorità giudiziarie straniere, tanto più ove l'atto di indagine sia compiuto in precedenza, nel corso di investigazioni da quest'ultima autonomamente

[20] Per tale ragione nel modulo prestampato, inviato alle autorità francesi, non risulta compilata la sezione "H7" riservata all'intercettazione di telecomunicazioni, né la sezione "H5" relativa ad «Atti di indagine che implicano l'acquisizione di prove in tempo reale, in modo continuo e per un periodo determinato».
[21] Cass., sez. V, 18 maggio 2016, n. 26885, in *www.dejure.it*
[22] Tribunale di Roma, Sezione del Riesame delle misure cautelari personali, Ord. 10 agosto 2022 «Le considerazioni che precedono valgono a maggior ragione nel caso in esame in quanto le richieste rogatoriali della Procura di Roma non hanno avuto ad oggetto attività investigativa da compiere, ma l'acquisizione di esiti di attività d'indagine che l'autorità straniera aveva già svolto, nel corso di autonome investigazioni e, per quanto dato conoscere nel rispetto della sua legislazione; fermo restando che tale atto, una volta introdotto nel procedimento italiano a seguito di relazioni rogatoriali, e quindi utilizzabile, sarà poi sottoposto a tutte le regole processuali e sostanziali proprie dell'ordinamento italiano, in particolare quanto alla valutazione del giudice del compendio delle acquisizioni documentali ed investigative ed alle possibilità di esercitare le prerogative difensive di tutela da parte dell'indagato».
Del medesimo tenore le argomentazioni spese dalla Corte di Assise di Roma, sentenza 9 giugno 2022 n. 7.

avviate, non possa essere condizionata, in forza del principio di reciproca fiducia, dall'accertamento da parte del giudice italiano della loro regolarità, vigendo, in primo luogo, una presunzione di legittimità dell'attività svolta e, poi, la verifica del giudice straniero circa la correttezza procedurale e l'eventuale risoluzione di ogni questione relativa alle irregolarità riscontrate[23]. L'assunto risulterebbe a maggior ragione valido poiché in materia di cooperazione giudiziaria in ambito dell'Unione Europea vige il principio del

[23] Cass., sez. II, 18 maggio 2010, n. 24776, in *www.dejure.it*: «L'utilizzazione degli atti non ripetibili compiuti dalla polizia straniera e acquisiti nel fascicolo per il dibattimento dopo l'esame testimoniale dell'autore degli stessi, ai sensi dell'art. 78, comma 2, disp. att. c.p.p., non è condizionata all'accertamento, da parte del giudice italiano, della regolarità degli atti compiuti dall'autorità straniera, vigendo una presunzione di legittimità dell'attività svolta e spettando al giudice straniero la verifica della correttezza della procedura e l'eventuale risoluzione di ogni questione relativa alle irregolarità riscontrate».
Ancora sul tema, Cass., Sez. V, 13 luglio 2016, n.45002, in *www.dejure.it*: «La sussistenza dei gravi indizi di colpevolezza richiesti per l'adozione di provvedimenti di cautela personale nella fase delle indagini preliminari può essere accertata anche mediante l'acquisizione della documentazione di atti compiuti autonomamente da autorità straniere in un diverso procedimento penale all'estero - anche al di fuori dei limiti stabiliti per la loro utilizzabilità dagli artt. 238 c.p.p. e 78 disp. att. c.p.p. - sempre che detta attività non si ponga in contrasto con norme inderogabili e principi fondamentali, che, però, non si identificano necessariamente con il complesso delle regole dettate dal codice di rito. Infatti, l'utilizzazione degli atti non ripetibili compiuti in territorio estero dalla polizia straniera e acquisiti nel fascicolo per il dibattimento non è condizionata all'accertamento, da parte del giudice italiano, della regolarità degli atti compiuti dall'autorità straniera - vigendo una presunzione di legittimità dell'attività svolta e spettando al giudice straniero la verifica della correttezza della procedura e l'eventuale risoluzione di ogni questione relativa alle irregolarità riscontrate - bensì alla compatibilità del diritto straniero sulla base del quale l'atto sia compiuto con i principi inderogabili dell'ordinamento interno, spettando, comunque, a colui che eccepisca il difetto di compatibilità darne la prova, tanto più ove si tratti di Paese membro dell'Unione Europea».

mutuo riconoscimento[24] che implica una presunzione di conformità (al sistema europeo) delle diverse legislazioni nazionali[25].
Alla luce delle considerazioni ed argomentazioni sin qui esposte apparrebbe dunque certa l'utilizzabilità del dato informatico così acquisito nel nostro ordinamento interno.
Se da una parte, infatti, non vi è dubbio che l'Autorità giudiziaria francese abbia agito nel pieno rispetto del codice di rito interno; d'altro lato

[24] Per una panoramica sul tema: S. Allegrezza, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello spazio giudiziario europeo*, in T. Rafaraci (a cura di), *L'area di libertà, sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia*, Atti del convegno, Catania, 9-11 luglio 2005, Milano, 2007, p. 691; L. Marin, *Il principio del mutuo riconoscimento nello spazio penale europeo*, Napoli, 2006, p. 78; R.M. Geraci, *Il mutuo riconoscimento nella cooperazione processuale: genesi, sviluppi, morfologie*, in *Giust. penale della post-modernità*, diretta da A. Scalfati -T. Bene – A. De Caro – G. Di Chiara – G. Garuti – S. Lorusso – M. Menna – N. Triggiani – D. Vigoni, Bari, 2020, p. 1 ss.; M. Perrotti, *Squadre investigative comuni in ambito euro unitario. Dalla decisione quadro alla normativa nazionale*, in *Dir. pen. proc*., 2016, p. 1008; V. Militiello, *Agli albori di un diritto penale comune in Europa: il contrasto al crimine organizzato*, in AA.VV., *Il crimine organizzato come fenomeno transnazionale. Forme di manifestazione, prevenzione e repressione in Italia, Germania e Spagna*, Milano, 2000, p. 16; M. Pisani, *Criminalità organizzata e cooperazione internazionale*, in *Riv. it. dir. proc. pen.*, 1998, p. 703; E. Selvaggi, *Criminalità transnazionale e cooperazione giudiziaria internazionale, in Criminalità transnazionale fra esperienze europee e risposte penali globali*, Atti del III Convegno internazionale promosso dal Centro studi giuridici "Francesco Carrara", Lucca 24-25 magio 2002, Milano, 2005, p. 417.

[25] Confermerebbero la piena legittimità delle attività compiute dall'Autorità francese alcune importanti pronunce d'oltre Alpe.
Il Conseil Costitutionnel 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, conferma la conformità costituzionale delle norme con riferimento all'art. 230, comma 1, c.p.p. francese, che consentono al Pubblico ministero, 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 all'acquisizione e all'estrapolazione dei dati, con l'effetto di schermare le informazioni relative a tali mezzi dal contraddittorio.
La Cour de Cassation con sentenza n. 00592 del 12 aprile 2022 respinge il ricorso, avverso la sentenza emessa dalla Corte di Appello di Parigi, proposto dai titolari di Sky Global (società fornitrice degli apparati telefonici criptati), confermando l'applicabilità della legge francese e la competenza dei tribunali francesi a giudicare gli imputati, in quanto: i due server appartenenti alla società in questione risulterebbero installati sul suolo nazionale (francese); il transito di tutte le conversazioni delle varie reti criminali avviene sul suolo transalpino; i rivenditori degli apparecchi telefonici Sky-Ecc vengono identificati in Francia; infine, gli utenti sono impegnati nel traffico di droga e nella trasformazione di denaro contante in bitcoin su suolo francese.

risulterebbero, altresì, pienamente rispettati i principi costituzionali sanciti dagli artt. 14 e 15 Cost. (libertà di domicilio e libertà e segretezza della corrispondenza e di goni altra forma di comunicazione); norme che, come è noto, consentono la violazione dei diritti fondamentali (solo) in presenza di atto motivato dell'Autorità giudiziaria[26].

4. Riflessioni.

A) La natura giuridica dei dati acquisiti.

Sebbene ad una prima lettura i provvedimenti che si stanno formando in materia paiono offrire valide e convincenti argomentazioni, meditando più attentamente sui temi posti a fondamento dell'impostazione esegetica sin qui analizzata pare potersi sostenere come gli stessi non soddisfino pienamente.

La soluzione evidenzia, infatti, come nella prassi giudiziaria odierna sia sempre più forte la tendenza a sacrificare le norme poste a presidio delle libertà fondamentali (e, dunque, del giusto processo) al precipuo scopo di reprimere (con qualsiasi mezzo) determinati fenomeni criminali.

Preliminarmente occorre operare una riflessione sulla natura giuridica del dato acquisito che, come già detto, viene catalogato nel novero dei documenti informatici ai sensi dell'art. 234-*bis* c.p.p.

È risaputo, che la norma viene introdotta, con il cd. "decreto antiterrorismo", dall'art. 2 L. 17 aprile 2015, n. 43.

La disposizione si inserisce in un quadro repressivo tipico della lotta al terrorismo nel quale, con strumenti legislativi eccezionali e di prevenzione, si tenta di rispondere all'utilizzo di sistemi tecnologici o informatici sempre più potenti ed in grado di criptare ogni tipo di comunicazione e nascondere ogni traccia di attività delittuosa[27].

L'art. 234-*bis* c.p.p. prevede due tipologie di acquisizione dati, in primo luogo, la libera acquisizione di dati informatici disponibili e fruibili attraverso la semplice navigazione in rete, trattandosi di dati che, per scelta consapevole o meno dell'interessato, sono condivisi da un numero indeterminato di

[26] Tribunale di Reggio Calabria, Sezione per il Riesame delle misure cautelari personali, Ord. 19 novembre 2022, n. 868, p. 8 «Invero, dalla lettura dei provvedimenti giudiziari francesi indentificati al n. D206, D207, 209-D, D209/1, D209/4, D210, D211/1, D212/1, D213/1 e D214/1 emessi dall'AG francese si evince che quest'ultima autorità abbia emesso specifici e motivati provvedimenti richiamando le norme del codice di procedura francese di "acquisizione di dati informatici" (giacenti/già presenti/conservati) riferibili alla piattaforma di chat SkyECC».

[27] S. Aterno, *L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nelle privacy*, in op.cit., p. 165.

soggetti[28]; poi, l'acquisizione di dati conservati all'estero e non liberamente fruibili.
In quest'ultima ipotesi ci si riferisce a tutti quei dati informatici che il titolare non ha voluto diffondere sulla rete e che ha inteso mantenere riservati su apposite piattaforme, alle quali è possibile accedere solamente con l'utilizzo di password o di cifrature.
In sede processuale questi dati sono utilizzabili unicamente se acquisiti con il "consenso del legittimo titolare".
Sebbene il concetto di titolare (del trattamento) sia richiamato nell'ambito del d.lgs. 196 del 2003 (Codice per la protezione dei dati personali), e l'art. 1 della L. 31 dicembre 1996, n. 675 stabilisce che per "titolare" debba intendersi" «*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali*», non esiste una definizione precisa in materia.
La carenza di specifici riferimenti normativi porta sia parte della dottrina[29], che la giurisprudenza (come già visto nel precedente paragrafo), ad interpretare estensivamente il concetto, affermando che legittimati ad esprimere il consenso sono un'amplia platea di soggetti che esercitano sui dati informatici diritti soggettivi (non si individua però una precisa tipologia di titolare o proprietario del dato).
Le ragioni di tale argomentare sarebbero essenzialmente due: da un lato, il concetto di titolare legato al trattamento dei dati personali sarebbe un concetto di derivazione europea che nasce con la direttiva sulla protezione dei dati personali 95/46 CE che potrebbe essere applicato solo sul territorio europeo e che, pertanto, non si applicherebbe a tutti quei soggetti e società che hanno sede e server fuori dall'ambito europeo; dall'altro, se il legislatore italiano avesse voluto far riferimento al "titolare" del trattamento ai sensi del codice privacy lo avrebbe fatto indicando espressamente tale normativa o quanto meno indicando il ruolo con il suo vero nome ovvero "titolare del trattamento" e non semplicemente "titolare" [30].
L'interpretazione offerta non convince per svariate ragioni.

---

[28] S. Aterno, *L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nelle privacy*, in op.cit., p. 165 «rientrano in questa categoria, ad esempio, i dati relativi ai profili pubblici sui social network, il contenuto di un sito web o di un blog, le fotografie pubblicate su piattaforme di condivisione a livello mondiale, i messaggi lasciati on line nei gruppi di discussione pubblici e altri dati simili. La caratteristica che hanno tutte queste informazioni è che per scelta consapevole (a volte inconsapevole) dell'interessato o dl proprietario del dato stesso, essi sono condivisi con una sfera indeterminata di soggetti».
[29] S. Aterno, *L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nelle privacy*, in op.cit., p. 165.
[30] S. Aterno, *L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nelle privacy*, in op.cit., p. 165.

Innanzitutto, avallando la tesi secondo cui il legislatore non circoscriverebbe appositamente l'ambito di applicazione della locuzione "legittimo titolare" varrebbe a minare in radice il principio di legalità (processuale) secondo cui le norme, com'è noto, devono connotarsi per la loro chiarezza e specificità.
Ragionando *a contrario*, peraltro, si potrebbe altresì sostenere che se il legislatore avesse voluto individuare una platea più ampia di persone portatrici di diritti soggettivi avrebbe certamente potuto operare un rinvio alle norme previste dal codice della privacy che definiscono il concetto di "titolare del trattamento".
Pertanto, dovendosi applicare quale criterio generale quello stabilito dall'art. 12 delle preleggi[31] secondo cui nell'applicare la legge non si può ad essa attribuire altro senso che quello fatto palese dal significato proprio delle parole, con il termine "legittimo titolare" non può che intendersi l'usuario del dispositivo che ha stipulato il contratto con la società di riferimento (SkyEcc).
Al più si potrebbe ipotizzare il consenso proveniente dal gestore del servizio (la società Sky Global) che ha, sia contratto apposito accordo con l'utente, sia la disponibilità dei dati informatici e delle chiavi di decriptazione.
Non a caso in passato la Suprema Corte di Cassazione[32], con riferimento ad altra tipologia di strumentazione criptata (i cd. dispositivi Blackberry), ammetteva implicitamente che per consenso di legittimo titolare potesse intendersi, al limite, quello derivante dal gestore del servizio: «*l'acquisizione della sequenza alfanumerica o simbolica (la cd. stringa) relativa alla messaggistica scambiata mediante sistema Blackberry, formatasi in territorio straniero, non necessita di rogatoria internazionale qualora, ai sensi dell'art. 234-bis c.p.p., vi sia il consenso del gestore straniero, dovendosi escludere in simili ipotesi la sanzione di inutilizzabilità dell'atto per violazione dell'atto*».
L'Autorità francese, dunque, non sembra potersi considerarsi in alcun modo titolare dei dati informatici in questione; potrebbe, al limite, essere la "detentrice" che li ha acquisiti (mediante installazione di un *malware* nei server di riferimento) coattivamente da uno dei legittimi titolari (l'azienda Sky Ecc) nell'ambito di una specifica attività d'indagine.
Rispetto alla natura giuridica del dato acquisito bisogna, poi, far "i conti" con quanto recentemente stabilito dalla Corte costituzionale con la sentenza n. 170/2023[33].
Con la pronuncia in esame la Consulta, accogliendo il conflitto di attribuzioni proposto dal Senato nei confronti della Procura della Repubblica presso il Tribunale di Firenze (il cd. "Caso Renzi") e, di fatto, stravolgendo

[31] Art. 12 Preleggi (intitolata «Interpretazione della legge»): «Nell'applicare la legge non si può ad essa attribuire altro senso che quello fatto palese dal significato proprio delle parole secondo la connessione di esse, e dalla intenzione del legislatore [...]».
[32] Cass., Sez. IV, 26 ottobre 20220, n. 49411, in *www.dejure.it*.
[33] C. cost., 27 luglio 2023, n. 170, in *www.cortecostituzionale.it*.

completamente l'orientamento giurisprudenziale sino ad oggi dominante in materia di *e-mail* e *whatsapp* (che attribuisce la natura documentale, ai sensi dell'art. 234 c.p.p., a tali forme di comunicazione)[34], propende nell'affermare, sulla falsa-riga di quanto già avvenuto in sede comunitaria dove da tempo si riconducono nell'alveo della corrispondenza tutelata dall'art. 8 C.E.D.U i messaggi informatico-telematici anche nella loro dimensione statica[35], che le summenzionate forme di comunicazione debbano rientrare nella nozione di «corrispondenza»[36].

Ciò in considerazione del fatto che la tutela dei precetti costituzionali non può esaurirsi con la ricezione del messaggio da parte del destinatario, ma deve perdurare fin tanto che esso conservi carattere di attualità e di interesse per gli interlocutori.

Per la Consulta il concetto di «corrispondenza» è ampiamente comprensivo, idoneo a contenere ogni comunicazione di pensiero umano tra due o più persone determinate, e si attua anche in modo diverso dalla conversazione *in itinere*.

Parafrasando una dottrina elaborata nell'ambito del diritto penale, con la locuzione forme di comunicazione si può intendere quell'insieme di rapporti psichici diretti, ancorché mediati, consistenti nella trasmissione di idee o di notizie, che una persona fa ad una o più altre persone determinate, col mezzo di cose atte a fissare, trasmettere e ricevere l'espressione del pensiero[37].

---

[34] Tra le varie Cass. civ., S.U, 27 aprile 2023, n. 11197 in *www.dejure.it* «In materia di procedimento disciplinare a carico dei magistrati, a sostegno di tale utilizzabilità, di messaggi whatsapp e gli sms conservati nella memoria del telefono cellulare, è stato più volte ribadito che gli stessi, hanno natura documentale ai sensi dell'art. 234 c.p.p., e come tali possono essere legittimamente acquisiti mediante la semplice riproduzione fotografica, non trovando applicazione in materia né la normativa sulle intercettazioni né quella sull'acquisizione della corrispondenza».

Cass. Sez. V, 14 febbraio 2023, in *www.dejure.it* «Gli sms, i messaggi whatsapp e di posta elettronica scaricati e/o conservati nella memoria dell'apparecchio cellulare, i messaggi pubblicati sul profilo facebook hanno natura di documenti ai sensi dell'art. 234 c.p.p. e, pertanto, con riferimento ad essi non trova applicazione né la disciplina delle intercettazioni, né quella relativa all'acquisizione di corrispondenza di cui all'art. 254 c.p.p.»

[35] C. edu, Copland c. Regno Unito, 3 aprile 2007, par. 44, in *www.europeanrights.com*; C. edu, Barbulescu c. Romania, 5 settembre 2017, par. 74, in *www.europeanrights.com*. Sul tema, F. Dinacci, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Proc. pen. giust.*, n. 2, 2022, p. 311 «Non è casuale, infatti, che la Corte comunitaria, ponendo l'accento sull'indispensabilità di individuare reati in ordine ai quali risulti assentibile l'acquisizione dei tabulati telefonici sia attratta nella disciplina della segretezza delle comunicazioni e comunque non sussumibile nello schema giuridico della prova documentale».

[36] Pertanto, ai sensi dell'art. 15 Cost., la loro limitazione potrà avvenire solo con atto motivato dell'autorità giudiziaria e con le forme e garanzie stabilite dalla legge.

[37] V. Manzini, *Diritto penale italiano*, VIII, Torino, 1947, p. 780.

Per determinare il concetto di comunicazione appare, infatti, del tutto irrilevante la materia o l'oggetto in cui si concreti il contenuto della stessa, sia la forma espressiva adoperata per trasmettere il pensiero (ad es. la lingua o segni), sia il mezzo di cui il soggetto si serve per consegnare il contenuto della comunicazione, consista esso (mezzo) negli ordinari servizi postali e di telecomunicazione, o in altri mezzi particolari.
Sebbene la portata del concetto di comunicazione debba risultare il più esteso possibile occorre tuttavia individuare, così come evidenzia la stessa Corte costituzionale, degli elementi determinativi indispensabili per circoscrivere l'ambito di tutela dell'art. 15 Cost.
La limitazione più saliente consiste, innanzitutto, nel carattere necessariamente inter-subiettivo o personale della comunicazione o della corrispondenza[38]: la comunicazione dev'essere formulata da un mittente che la fa pervenire nella sfera di conoscenza di uno o più destinatari.
Un secondo limite è rappresentato, poi, dall'«attualità» della comunicazione: una comunicazione non sarà più attuale «quando, ormai, per il decorso del tempo o per altra causa non gli si può assegnare (alla comunicazione o alla corrispondenza) che un valore meramente retrospettivo, affettivo, collezionistico, storico, artistico, scientifico o probativo»[39].
Chiarito dunque, seppur sinteticamente, l'ambito e la portata della tutela del concetto di corrispondenza-comunicazione, evidenti appaiono le ragioni che inducono la Corte costituzionale ad esprimersi nei seguenti termini[40]:
«*La tesi della resistente – che porterebbe al rigetto del ricorso, in quanto non si sarebbe di fronte a una ipotesi di sequestro di corrispondenza, ma a una mera*

[38] A. Pace, *Sub* Art. 15, *Commentario della Costituzione*, a cura di G. Branca, *Rapporti Civili art. 13- 20*, Bologna, 1977, p. 82 «La protezione della socialità dell'uomo – l'invito cioè a collegarsi coi propri simili, corrispondendo e comunicando con loro, nonché la garanzia che tali espressioni del pensiero possano liberamente giungere al destinatario (nel che si sostanzia la libertà in questione) – viene assunta come aspetto inviolabile della persona umana. E la constatazione che con l'articolo in esame si sia in parte disciplinata la stessa libertà sostanziale di espressione del pensiero diviene significativa. L'assenza, nell'art. 15 Cost., di limiti sostanziali e di poteri preventivi di polizia testimonia come la tutela della socialità dell'uomo non implichi, per la Costituzione, che tale libertà possa dirsi funzionalizzata al perseguimento di valori connessi a valutazioni di pubblico interesse.
In altre parole: la circostanza che un fatto sociale come la comunicazione nelle sue varie forme sia ritenuto inviolabile e venga sottratto al condizionamento dei valori propri della collettività, comprova l'esattezza di ciò: che una cosa è affermare la rilevanza sociale di una libertà, altra e ben diversa è dedurre, dalla necessaria inter-subiettività della sua attuazione, l'immanenza di un vincolo funzionale al perseguimento di finalità d'ordine sociale.
[39] V. Manzini, *Diritto penale italiano*, op. cit., p. 780.
[40] M. Borgobello, *Il concetto di corrispondenza nella sentenza 170 del 2023 della Corte costituzionale*, in *Giur. Pen. web,* n. 8, 2023, p. 5.

e generica acquisizione di documenti, non rientrante nel novero degli atti per i quali l'art. 68 Cost. esige il placet della Camera di appartenenza del parlamentare – non può essere condivisa.
Degradare la comunicazione a mero documento quando non è più in itinere, è soluzione che, se confina in ambiti angusti la tutela costituzionale prefigurata dall'art. 15 Cost. nei casi, sempre più ridotti, di corrispondenza cartacea, finisce addirittura per azzerarla, di fatto, rispetto alle comunicazioni operate tramite posta elettronica e altri servizi di messaggistica istantanea, in cui all'invio segue immediatamente – o, comunque sia, senza uno iato temporale apprezzabile – la ricezione. […]
Questa Corte, d'altronde, ha già da tempo affermato che la garanzia apprestata dall'art. 15 Cost. si estende anche ai dati esteriori delle comunicazioni (quelli, cioè, che consentono di accertare il fatto storico che una comunicazione vi è stata e di identificarne autore, tempo e luogo): problema postosi in rapporto ai tabulati telefonici, contenenti l'elenco delle chiamate in partenza o in arrivo da una determinata utenza.
In proposito si è rilevato che la stretta attinenza della libertà e della segretezza della comunicazione al nucleo essenziale dei valori della personalità – attinenza che induce a qualificare il corrispondente diritto "come parte necessaria di quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana" – comporta un particolare vincolo interpretativo, diretto a conferire a quella libertà, per quanto possibile, un significato espansivo».
È per tali ragioni (ed è forse questo il passaggio della sentenza che maggiormente rileva ai fini della presente ricerca) che, prosegue la Corte, le tutele accordate dagli artt. 15 e 68, terzo comma, Cost. debbono estendersi, contrariamente a quanto sostiene l'orientamento che si sta andando a consolidare in materia di telefonia criptata («*L'acquisizione, previa decriptazione, tramite ordine europeo di indagine, dall'autorità francese di comunicazioni acquisite sui server delle piattaforme "Encrochat" e "Sky-Ecc" è disciplinata dall'articolo 234 bis c.p.p., che consente "l'acquisizione di documenti e dati informatici conservati all'estero", dovendosi escludere, invece, l'applicabilità della disciplina degli articoli 266 e ss. c.p.p., che è destinata ad operare solo con riferimento a flussi di comunicazioni in atto*»)[41], anche al sequestro di messaggi elettronici, quand'anche già recapitati al destinatario («*Ma se, dunque, l'acquisizione dei dati esteriori di comunicazioni già avvenute (quali quelle memorizzate in un tabulato) gode delle tutele accordate dagli artt. 15 e 68, terzo comma, Cost., è impensabile che non ne fruisca, invece, il sequestro di messaggi elettronici, anche se già recapitati al destinatario: operazione che consente di venire a conoscenza non soltanto dei dati identificativi estrinseci delle comunicazioni, ma anche del loro contenuto, e dunque di attitudine intrusiva tendenzialmente maggiore*»).

[41] Cass., Sez. IV, 5 aprile 2023, n. 16345, in *www.dejure.it*.

Cercando di tirare le somme, appare evidente come le argomentazioni sin qui svolte facciano emergere più di qualche dubbio e perplessità rispetto alla natura documentale-informatica attribuita alla messaggistica SkyEcc dall'impostazione esegetica che si sta consolidando in materia.
Non solo infatti, come ampiamente detto, sembrerebbe difettare il requisito del consenso del legittimo titolare richiesto dall'art. 234-*bis* c.p.p.; ma inoltre, stando alle recenti indicazioni offerte dalla sentenza della Corte costituzionale, sembrerebbe opportuno far ricadere l'attività di acquisizione delle chat nell'ambito della disciplina (maggiormente garantita) prevista in materia di intercettazioni di cui agli artt. 266 e 266-*bis* c.p.p.
A tal riguardo, si ricorda peraltro come già in passato la stessa Corte di Cassazione, proprio in tema, dapprima di *e-mail* e poi di chat Blackberry, riteneva che l'acquisizione dei messaggi già spediti o ricevuti dall'indagato, e conservati nelle rispettive caselle di entrata e uscita o nei server Blackberry situati in Canada, potesse costituire vera e propria attività di intercettazione.
In tale sede, infatti, si affermava che il discrimine affinché vi fosse o meno un flusso informatico – e quindi dovesse essere applicata la disciplina delle intercettazioni – risiedeva nell'avvenuto inoltro del messaggio da parte del mittente[42] («*È legittima l'acquisizione di contenuti di attività messaggistica - nella specie, effettuata con sistema Blackberry - mediante intercettazione operata ai sensi degli artt. 266 ss. c.p.p., poiché le chat, anche se non contestuali, costituiscono un flusso di comunicazioni*»).
Aderendo a tale impostazione esegetica, naturali dovrebbero apparire le ripercussioni sul fronte della inutilizzabilità processuale dei dati SkyEcc acquisiti, ai sensi dell'art. 234-*bis* c.p.p., tramite ordine europeo di indagine:

[42] Cass. Sez. III, 10 novembre 2015, n. 50452, in *C.E.D. Cass*, n. 265615; Cass. Sez. IV, 28 giugno 2016, n. 40903, in *C.E.D. Cass.*, n. 268228.
Tale orientamento sembrerebbe trovare conferma in una risalente pronuncia delle Sezioni Unite, 13 luglio 1998, Gallieri, in *C.E.D. Cass*, n. 211197, con cui si invitava a valutare appieno la portata innovativa della l. 23 dicembre 1993, n. 547 sui computer crimes, con cui è stato introdotto l'art. 266-*bis* c.p.p.
La sentenza Gallieri ha infatti evidenziato che la telefonia, in specie mobile, consente il trasporto di segnali non solo relativi alle conversazioni, ma di qualunque tipo, sempre in forma numerica, cioè di dati diversi dal contenuto delle conversazioni telefoniche. E di tali dati deve attualmente ritenersi consentita l'intercettazione in virtù proprio dell'art. 266-*bis* c.p.p.
Per completezza si segnala l'esistenza anche di un orientamento di segno contrario, Cass., pen. sez. VI, 28 maggio 2019, n.28269, *in* www.dejure.it; Cass., Sez. VI, 6 febbraio, 2020, n.12975, in Cass. Pen., 2020, 12, p. 4664 «In tema di mezzi di prova, i messaggi di posta elettronica memorizzati nell'account o nel computer del mittente ovvero del destinatario hanno natura di documenti informatici, sicché la loro acquisizione processuale non soggiace alla disciplina delle intercettazioni di cui all'art. 266-bis c.p.p., che postula la captazione di un flusso di comunicazioni in atto, ma avviene ai sensi dell'art. 234 c.p.p.».

in primo luogo, per la violazione dell'art. 15 Cost. secondo cui la limitazione delle comunicazioni può avvenire solo nei casi e modi previsti dalla legge[43] e per atto motivato dell'autorità giudiziaria; dunque, per la conseguente e totale elusione delle norme previste in materia di intercettazioni.
Pertanto, essendo noto come il momento di valutazione dell'utilizzabilità della prova estera non può che avvenire secondo le regole dettate dall'ordinamento in cui quella prova è chiamata ad esprimere il suo contenuto conoscitivo[44], ne consegue che il giudice italiano avrebbe dovuto vanificarne il risultato, poiché la prova (così acquisita dalla Francia) si pone in aperto contrasto con i principi dell'ordinamento nazionale.
Del resto, così come afferma autorevole dottrina, la circostanza «appare tanto più rilevante ove si consideri che la materia probatoria risulta intimamente connessa al profilo dei diritti e delle garanzie difensive, che non possono essere sacrificati per il solo fatto che l'assunzione probatoria abbia luogo in territorio straniero piuttosto che nello Stato in cui pende il procedimento»[45].

---

[43] La riserva di legge, come è noto, è funzionale a contenere il potere discrezionale del magistrato e, al contempo, scongiurare il rischio di eventuali abusi da parte degli organi inquirenti.
Per una panoramica sulla riserva di legge: P. Costa, *Lo Stato di diritto: un'introduzione storica,* in P. Costa – D. Zolo (a cura di), *Lo Stato di diritto*, Milano, 2002, p. 94; C.S. Montesquieu, *Lo spirito delle leggi,* 1748, ed. a cura di G. Carnazzi, con prefazione di V. Grevi, Milano, 2010; R. Bin – G. Petruzzella, *Diritto Costituzionale*, Torino, 2011, p. 325.

[44] F.R. Dinacci, *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, op. cit., p. 144 «La prospettiva non si pone in contrasto con l'obbligo di osservanza della lex loci stabilito dall'art. 3, comma 1, della Convenzione europea di assistenza giudiziaria. Tale obbligo, infatti, non viene violato dal momento che l'assunzione della prova all'estero viene effettuata secondo le regole di quello Stato. Ma la situazione, risulta evidente, non preclude alla giurisdizione utilizzatrice delle prove estere un giudizio sulla legalità delle forme assuntive. Del resto, tale possibilità è ribadita dalla stessa rilevanza della legge del luogo, la quale non potrà che essere quella nell'ambito del quale il dato conoscitivo viene utilizzato».
Sul punto anche, Cass. Sez. I, 18 gennaio 1971, n. 33, in *www.dejure.it* «Le prove raccolte all'estero sono ammissibili in un giudizio che si svolge in Italia, sempre che si tratti di prove legalmente assunte quanto alla forma, in conformità della legge del luogo ove sono state raccolte, e non siano in contrasto con le nostre leggi proibitive concernenti le persone e gli atti o con quelle che, in qualsiasi modo, riguardino l0ordine pubblico. L'efficacia giuridica di tali prove è valutata secondo le disposizioni della legge italiana ed alla parte interessata incombe l'obbligo di dimostrare la non rispondenza dell'atto con la legge estera, mediante la produzione della legge penale straniera».

[45] M.R. Marchetti, *L'assistenza giudiziaria internazionale*, Milano, 2005, p. 43.

B) L'incompatibilità con le indicazioni provenienti dalla Corte di Giustizia Europea.

Nel secondo paragrafo si è chiarito come la piattaforma SkyEcc offre in dotazione agli utenti, come ulteriore forma di «protezione», sim-card di sua proprietà che non consentono di risalire (immediatamente) ai proprietari degli apparecchi mobili.

L'anonimato garantito dalle schede telefoniche non impedisce, tuttavia, all'organo inquirente di venire a conoscenza del luogo di utilizzo (e dunque, verosimilmente, anche degli utilizzatori) dei sistemi crittografici.

La tecnologia in questione, infatti, sfruttando la convenzionale rete telefonica per inviare i messaggi, coinvolge, come ogni altro sistema di comunicazioni, le consuete celle nazionali.

Agganciando una data cella, le sim-card inserite nei diversi dispositivi «rilasciano» una serie di dati (i cd. dati esteriori di comunicazioni), tra cui il codice IMSI ed IMEI che, nelle diverse operazioni investigative di cui si discute, vengono acquisiti dai diversi organi inquirenti nazionali per fini di polizia.

I dati telefonici raccolti dagli investigatori italiani (i codici IMSI ed IMEI), incrociati con la massa delle risultanze probatorie fornite dall'Autorità giudiziaria francese (i messaggi già decodificati), rendono possibile l'individuazione dei numerosi utilizzatori e possessori degli apparecchi telefonici criptati SkyEcc.

Quantomeno sul fronte interno, l'attività di acquisizione dei dati in questione così realizzata pare cadere in conflitto, oltre che con le garanzie previste dall'art. 15 Cost., anche con le indicazioni provenienti dalla Corte di Giustizia Europea in materia di intangibilità della riservatezza delle comunicazioni.

È circostanza nota che con la tradizionale locuzione «dati esteriori di comunicazioni» si intende far riferimento ad una serie di informazioni di varia natura, suscettibili di acquisizione e di utilizzazione processuale, che riguardano non solo i dati relativi alle telefonate su apparecchi fissi o mobili, ma anche ogni altro tipo di comunicazione elettronica.

Si tratta di dati personali qualificati perché forniscono retrospettive di indubbio rilievo quali il tempo, la durata, la frequenza delle chiamate, le utenze contattate, i codici IMEI, gli intestatari delle SIM e l'ubicazione dell'utenza mediante la geolocalizzazione storica delle celle di aggancio, consentendo così di creare una mappatura fedele ed esaustiva di una parte importante dei comportamenti privati di una persona.

È proprio in ragione della loro capacità intrusiva che la Corte costituzionale, già con la sentenza n. 81 del 1993, riconosceva, in forza dell'art. 15 Cost., il diritto di mantenere segreti tanto i dati che possono portare

all'identificazione dei soggetti della conversazione, quanto quelli relativi al tempo e al luogo della comunicazione[46].
La Corte, tuttavia, ravvisando che l'acquisizione dei dati esteriori comprimesse in maniera sensibilmente minore il diritto di cui all'art. 15 Cost. rispetto alla tradizionale captazione delle conversazioni, riteneva sufficiente procedere all'acquisizione del dato attraverso l'emissione di un decreto motivato del pubblico ministero, mutuando così la disciplina stabilita per il sequestro di corrispondenza.
Sulla scorta di tale pronuncia ne susseguivano altre che, ripercorrendo e riprendendo le argomentazioni offerte dalla sentenza n. 81 del 1993, confermano e ribadiscono i principi espressi in precedenza[47].

---

[46] C. cost., sentenza 11 marzo 1993, n. 83, in *www.cortecostituzionale.it*, massima n. 19298 «Non è contestabile che l'art. 15 della Costituzione, in mancanza delle garanzie ivi previste, preclude la divulgazione o, comunque, la conoscibilità da parte di terzi delle informazioni e delle notizie idonee a identificare i dati esteriori della conversazione telefonica (autori della comunicazione, tempo e luogo della stessa), dal momento che, facendone oggetto di uno specifico diritto costituzionale alla tutela della sfera privata attinente alla libertà e alla segretezza della comunicazione, ne affida la diffusione, in via di principio, all'esclusiva disponibilità dei soggetti interessati. Né, al tempo stesso, può negarsi che al riconoscimento di tale diritto, sempre in forza all'art. 15 della Costituzione, sia co-essenzialmente legata la garanzia consistente nel dovere, posto a carico di tutti coloro che per ragioni professionali vengano a conoscenza del contenuto e dei dati esteriori della comunicazione, di mantenere il più rigoroso riserbo sugli elementi suddetti. Pertanto, anche se la tutela relativa alla riservatezza dei dati di identificazione in questione non si è finora tradotta in specifiche norme processuali, l'acquisizione come mezzi di prova dei medesimi non può non avvenire nel più rigoroso rispetto delle regole che la stessa Costituzione pone direttamente, e cioè soltanto sulla base di un atto dell'autorità giudiziaria sorretto da un'adeguata e specifica motivazione, diretta a dimostrare la sussistenza in concreto di esigenze istruttorie volte al fine, costituzionalmente protetto, della prevenzione e della repressione dei reati. Ferma restando la libertà del legislatore di stabilire più specifiche norme di attuazione di tali principi costituzionali, il ricordato livello minimo di garanzie pone dunque un parametro di validità che spetta al giudice "*a quo*" applicare direttamente al caso di specie.»
[47] C. cost., sentenza 28 maggio n. 2010, n. 188, in *www.cortecostituzionale.it*; C. cost., 6 marzo 2019, n. 38, in *www.cortecostituzionale.it*, massima n. 42192 «Il duplice riferimento testuale, nell'art. 68, terzo comma, Cost., a "conversazioni o comunicazioni" induce a ritenere che al contenuto di una conversazione o di una comunicazione siano accostabili, e risultino perciò protetti dalla garanzia costituzionale, anche i dati puramente storici ed esteriori, in quanto essi stessi "fatti comunicativi".
La previsione censurata, equiparando ai fini del suo utilizzo in giudizio il tabulato telefonico alla registrazione o al verbale di un'intercettazione, non lede pertanto il principio di uguale soggezione alla legge, ma attua il pertinente trattamento richiesto dalla garanzia costituzionale che mira a proteggere la libertà della funzione che il soggetto esercita, e per questa ragione può estendersi ad un atto investigativo

In materia di intangibilità della riservatezza delle comunicazioni passi decisamente più marcati vengono compiuti in sede comunitaria.
In particolare, è la Corte di Giustizia, in linea con le pronunce della Corte Europea dei diritti dell'Uomo[48], ad individuare precisi limiti per l'acquisizione dei dati in questione.
Approfondendo i principi già affermati in materia di *data retention*[49], la Grande Sezione della Corte di Giustizia, con la sentenza del 2 marzo 2021, H.K. c. Prokunrantuur, pronunciandosi sul rinvio pregiudiziale formulato dalla Corte Suprema estone in ordine all'interpretazione dell'art. 15, par. 1, dir. 2002/58/CE – relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche – come modificata dalla direttiva 2009/136/CE del Parlamento Europeo e del Consiglio, del 25 novembre 2009 – delinea una serie di linee-guida a cui gli Stati membri devono soggiacere per consentire l'accesso da parte dell'autorità pubblica ai dati conservati dai fornitori.
Tali limiti sono chiaramente introdotti al fine di bilanciare esigenze di prevenzione, accertamento e repressione dei reati con la contrapposta, ma necessaria, tutela del diritto alla riservatezza dei cittadini[50].
La pronuncia in esame afferma a chiare lettere che la direttiva 2009/136/CE, letta alla luce degli artt. 7, 8 e 11 nonché dell'art 52, par. 1, della Carta dei diritti fondamentali dell'Unione Europea, osti: da un lato, a una normativa nazionale che consenta alle autorità pubbliche l'accesso a dati relativi al traffico o a dati relativi all'ubicazione – dunque idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o, come nel caso di specie, sull'ubicazione delle apparecchiature terminali da costui utilizzate – per finalità di prevenzione, ricerca, accertamento e perseguimento dei reati senza che tale accesso sia circoscritto a procedimenti aventi per scopo la lotta contro forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza.
Dall'altro, a una normativa nazionale che investa il pubblico ministero della competenza ad autorizzare l'accesso ai dati relativi al traffico e ai dati relativi

idoneo a incidere sulla libertà di comunicazione del parlamentare, qual è certamente il tabulato, che, per la sua pervasività, può tradursi in fonte di condizionamento sul libero esercizio della funzione. (*Precedenti citati: sentenze n. 188 del 2010, n. 114 del 2010, n. 113 del 2010, n. 390 del 2007, n. 281 del 1998, n. 81 del 1993 e ordinanza n. 263 del 2010*) ».

[48] C. edu, Copland c. Regno Unito, 3 aprile 2007, par. 44, in *www.europeanrights.com*; C. edu, Barbulescu c. Romania, 5 settembre 2017, par. 74, in www.europeanrights.com.

[49] Corte di Giustizia, Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB*; Corte Giustizia, Grande Sezione 8 aprile 2014, cause riunite C-293/12 e C-594/12 *Digital Right Ireland*.

[50] Sul tema A. Malacarne -G. Tessitore, *La ricostruzione della normativa in tema di data retention e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?* in *Arch. pen.*, 2022, n. 3, p. 25.

all'ubicazione (così come, invece, ritiene la Corte costituzionale con le pronunce sopra richiamate) al fine di condurre un'istruttoria penale.
Per tali ragioni, prosegue la Corte di Giustizia, è necessario che il controllo preventivo venga (necessariamente) rimesso a un giudice o a un'autorità amministrativa indipendente e terza rispetto alle parti pubbliche e private.
Tutto ciò al duplice fine, sia, di evitare che pratiche illegittime di acquisizione di dati, o la loro conservazione generalizzata ed indifferenziata[51], possano arrecare pregiudizio a una o più persone che, in quel dato momento storico, ben potrebbero non essere sospettate (neppure indiziate) di aver commesso reati; sia, di escludere informazioni ottenute in violazione delle prescrizioni del diritto dell'Unione che sono funzionali a garantire il rispetto del principio del contraddittorio e, dunque, del diritto ad un equo processo.
La Corte di Giustizia così facendo introduce, come afferma autorevole dottrina, una "nuova" forma di inutilizzabilità di «derivazione comunitaria che, all'evidenza, si affianca a quelle scaturenti dalla violazione dei principi costituzionali»[52] che impone ai giudici nazionali di escludere dal compendio probatorio informazioni ed elementi di prova ottenuti illegittimamente (e/o conservati in maniera generalizzata e indifferenziata)[53].

---

[51] F. Dinacci, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *op. cit.*, p. 314.
[52] F. Dinacci, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *op. cit.*, p. 314. Ancora sul tema, S. Marcolini, *Le indagini atipiche nel processo penale*: una proposta, in *Cass. pen.*, 2015, p. 775
[53] È proprio sulla scorta dei principi enunciati dalla Corte di Giustizia che il legislatore italiano adotta il D.L. 30 settembre 2021, n. 132 (Misure urgenti in materia di giustizia e difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP entrato in vigore il 30 settembre 2021) con cui si evidenzia la straordinaria necessità (ed urgenza) di garantire la possibilità di acquisire dati relativi al traffico telefonico e telematico per fini di indagine penale nel rispetto dei principi enunciati dalla Grande Sezione della Corte di Giustizia dell'Unione Europea, e in particolare di circoscrivere le attività di acquisizione ai procedimenti penali aventi ad oggetto forme gravi di criminalità e di garantire che dette attività siano soggette al controllo di un'autorità giurisdizionale.
L'art. 1 del decreto-legge, intitolato "Disposizioni in materia di acquisizione dei dati di traffico telefonico e telematico per fini di indagine penale", ha riscritto l'art. 132, comma 3, del d.lgs. n. 30 giugno 2003, n. 196, prevedendo che "entro il termine di conservazione imposto dalla legge se sussistono sufficienti indizi di reato per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tra anni determinata a norma dell'art. 4 c.p.p., e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti ai fini della prosecuzione delle indagini, i dati sono acquisiti presso il fornitore con decreto motivato del giudice su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta ad indagini, della persona offesa o delle altre parti private".

Ora, in considerazione di quanto sin qui detto, appare opportuno rivalutare le argomentazioni utilizzate dai giudici italiani, tese a provare (*rectius,* giustificare) la legittimità delle procedure poste in essere per l'acquisizione dei dati sottoforma di documentazione informatica, anche alla luce dei criteri offerti dalla Corte di Giustizia.

Se da un lato, infatti, appare vera la circostanza secondo cui risulterebbero esistere "a monte" i provvedimenti autorizzativi di un Giudice francese[54] per le intercettazioni telefoniche («*Invero, dalla lettura dei provvedimenti giudiziari francesi indentificati al n. D206, D207, 209-D, D209/1, D209/4, D210, D211/1, D212/1, D213/1 e D214/1 emessi dall'AG francese si evince che quest'ultima autorità abbia emesso specifici e motivati provvedimenti* […])»; dall'altro canto, non si può revocare in dubbio come i provvedimenti autorizzativi emessi dai Giudici di Lille e di Parigi non riguarderebbero affatto l'intera massa delle captazioni (tra cui, appunto, quelle per cui oggi si procede in Italia), bensì esclusivamente una serie di comunicazioni afferenti reati di criminalità organizzata e terrorismo compiuti in Francia nell'anno 2021.

La circostanza non appare di poco momento poiché evidenzia come, ad eccezione di alcune conversazioni, la gran parte della messaggistica viene acquisita in assenza di una notizia di reato, in mancanza dei relativi provvedimenti autorizzativi e, viene conservata su appositi server in maniera del tutto generalizzata ed indifferenziata.

In considerazione di quanto sin qui detto si ritiene dunque, innanzitutto, che i giudici francesi avrebbero dovuto procedere, immediatamente e compatibilmente con le indicazioni comunitarie, alla cancellazione dal server di convoglio di tutte le chat per cui non c'è autorizzazione alle intercettazioni.

Del resto, anche la disciplina francese prevista in materia di intercettazioni, analogamente a quella italiana, detta una rigida disciplina prevedendo che l'autorizzazione emessa dal Giudice istruttore indichi tassativamente: gli elementi necessari ad identificare le comunicazioni passibili di captazione; il reato in relazione al quale è disposta l'attività di ricerca della prova; la relativa durata (ciò indipendentemente se si procede nelle forme previste dall'art. 100 c.p.p. francese o 706-102-1 c.p.p. francese, nella sua formulazione risultante dalla legge 23 marzo 2019) dell'attività di captazione[55].

---

[54] Tribunale di Reggio Calabria, Sezione per il Riesame delle misure cautelari personali, Ord. 19 novembre 2022, n. 868, p. 8 «Invero, dalla lettura dei provvedimenti giudiziari francesi indentificati al n. D206, D207, 209-D, D209/1, D209/4, D210, D211/1, D212/1, D213/1 e D214/1 emessi dall'AG francese si evince che quest'ultima autorità abbia emesso specifici e motivati provvedimenti richiamando le norme del codice di procedura francese di "acquisizione di dati informatici" (giacenti/già presenti/conservati) riferibili alla piattaforma di chat SkyECC».

[55] Art. 100 c.p.p. francese «In materia penale e correzionale, se la pena inflitta è pari o superiore a tre anni di reclusione, il giudice istruttore può, quando le esigenze dell'informazione lo richiedono, prescrivere l'intercettazione, la registrazione e la

Poi, non essendo la cancellazione della messaggistica avvenuta, si sarebbe attesa dai giudici nazionali una declaratoria di inutilizzabilità della messaggistica SkyEcc, oltre che per l'incompatibilità delle procedure acquisitive poste in essere dall'autorità giudiziaria transalpina con le norme inderogabili dell'ordinamento interno, per la violazione, appunto, dei principi sanciti dalla Corte di Giustizia in materia di intangibilità delle comunicazioni.

C) SkyEcc e principio del contraddittorio.

Come già accennato, l'Autorità giudiziaria francese, ricevuti gli Ordini d'Indagine Europei dai diversi uffici di Procura italiani, trasmette i CD-ROM contenenti la messaggistica SkyEcc già decriptata senza, tuttavia, nulla specificare né in ordine alle modalità di acquisizione dei dati, né a quelle di decriptazione.

Sebbene l'orientamento che si sta consolidando in materia affermi che la mancata indicazione da parte dell'Autorità giudiziaria francese dei criteri di decifrazione dei flussi di comunicazioni non può tradursi di per sé in un'alterazione del dato originale (ciò in considerazione del fatto che, da un lato, l'algoritmo indispensabile per trasformare il messaggio "in chiaro" non può in alcun modo alterare il contenuto, trattandosi di un'operazione "*on/off*" mediante cui o si traduce tutto il corpo del testo o non si decifra nulla; dall'altro per il principio "*locus regit actum*", e in conformità ai canoni di diritto internazionale, prevale la "*lex loci*" - quella francese - sulla "*lex fori*" - quella italiana - e, pertanto, le concrete modalità di assistenza difensiva sarebbero regolate dalla legge dello Stato in cui l'atto viene compiuto) e, dunque, incidere sull'utilizzabilità processuale dei dati in oggetto; chi scrive ritiene invece che simile modo di procedere contrasti apertamente con il principio del contraddittorio di cui all'art. 111 Cost.

Tali considerazioni vengono inizialmente condivise dalla Suprema Corte di Cassazione che, chiamata ad esprimersi per la prima volta sull'argomento[56] (e prima di stravolgere completamente la propria impostazione esegetica), stabilisce come le procedure acquisitive della messaggistica SkyEcc così realizzate non sono compatibili con le norme inderogabili e i principi fondamentali del nostro ordinamento giudiziario.

---

trascrizione della corrispondenza inviata per via telematica comunicazioni. Queste operazioni sono svolte sotto la sua autorità e controllo [...]».

Art. 706-102-1 c.p.p. francese, nella sua formulazione risultante dalla legge 23 marzo 2019 «Si può ricorrere all'attuazione di un dispositivo tecnico il cui scopo, senza il consenso degli interessati, è quello di accedere, ovunque, a dati informatici, di registrarli, archiviarli e trasmetterli, in quanto conservati in un sistema informatico, come vengono visualizzati su uno schermo dall'utente di un sistema automatizzato di elaborazione dati , poiché li introduce inserendo dei caratteri o mentre vengono ricevuti e inviati dalle periferiche».

[56] Cass., sez. IV, 15 luglio 2022, n. 32915, in *Guida al diritto*, 2022, p. 38

A tal riguardo, il Supremo Collegio afferma che: «*in relazione all'utilizzabilità processuale, anche in sede cautelare, della messaggistica acquisita da Europol, tramite il coordinamento delle attività delle polizie francese, belga e olandese, attraverso l'accesso ai server di Sky ECC (sistema di produzione canadese, specializzata nella fornitura di strumenti di comunicazione sicura e protetta da un sistema di codifica dei dati) che la conservavano in memoria, non è sufficiente la formale acquisizione della messaggistica tramite ordine europeo di indagine, ma occorre il riscontro di conoscenza delle modalità di acquisizione del detto materiale, perché è necessario valutare, nell'ambito del procedimento che tali modalità di acquisizione della messaggistica non siano in contrasto con norme inderogabili e principi fondamentali del nostro ordinamento.*
Infatti, il principio del contraddittorio implica che la dialettica procedimentale deve esplicarsi non soltanto relativamente al vaglio del materiale acquisito, ma si deve estendere anche alle modalità di acquisizione del predetto materiale.
Ciò è funzionale al controllo della legittimità del procedimento acquisitivo, anche nell'ottica delineata dall'articolo 191 del c.p.p., il quale stabilisce l'inutilizzabilità delle prove acquisite in violazione dei divieti stabiliti dalla legge.
Le modalità di acquisizione del materiale probatorio rilevano, inoltre, nell'ottica della valutazione della valenza epistemica di quest'ultimo, sotto il profilo della corrispondenza della testualità di tale messaggistica al tenore letterale dei messaggi originariamente inviati e ricevuti nonché delle utenze dei mittenti e dei destinatari individuati con quelli effettivi, ragion per cui la problematica in disamina dispiega la propria rilevanza anche relativamente alle fasi della captazione e della decrittazione dei flussi telematici».
Ad avviso di chi scrive, già dalla semplice lettura della massima, pare possibile rilevare come la pronuncia colga nella sua interezza il significato e la portata del principio di cui all'art. 111 Cost[57].
Il contraddittorio, come è noto, non verte solo sull'oggetto da provare, bensì anche su tutte le attività intese a farlo[58].
Non a caso la dottrina[59] è da tempo orientata in tal senso, affermando che il principio in questione si presenti come una sorta di *work in progress*, che si

[57] Art. 111 Cost. «La giurisdizione si attua mediante il giusto processo regolato dalla legge. Ogni processo si svolge nel contraddittorio tra le parti, in condizioni di parità, davanti a un giudice terzo ed imparziale. La legge ne assicura la ragionevole durata».
[58] G. Conso, *Considerazioni in tema di contraddittorio nel processo penale italiano*, in *Riv. it. dir. e proc. pen*., 1966, p. 405 ss. «Ogni forma di contraddittorio presuppone una dualità antagonistica e paritetica, nel senso che i suoi protagonisti debbono essere portatori di interessi e obbiettivi diversi, anche se nella disputa possono trovare uno o più punti di convergenza, e debbono godere di equivalenti diritti. Primo fra tutti, tanto da doverlo considerare un presupposto di esistenza del contraddittorio, quello di conoscere compiutamente l'oggetto del contendere».
[59] F. Cordero, *Riti e sapienza del diritto*, Bari, 1981, p. 433.

snoda lungo una sequela di atti, il primo dei quali (domanda, imputazione) pone il tema della contesa e l'ultimo (la sentenza) la risolve.
La pluralità dei momenti dialettici – aventi un'autonomia logica, ma non funzionale – confluisce nell'unità teleologica che tutti li ispira: la comune tensione verso un risultato finale, dal contenuto variabile, secondo l'interesse che ciascun contendente persegue[60].
Alla luce di ciò, appare dunque chiaro ed evidente come l'impossibilità per le difese di conoscere i messaggi di testo in originale, le procedure di acquisizione da parte dell'Autorità francese e, infine, le modalità di decriptazione delle conversazioni oggetto di intercettazioni, si traduca in una forte ed irragionevole compromissione del suddetto principio.
Non solo, infatti, gli indagati-imputati non sono posti nelle condizioni di esercitare il proprio diritto di difesa sulla scorta di un preteso segreto di Stato francese[61] che li obbliga ad accettare "al buio" i dati trasmessi tramite O.I.E. (la prassi giudiziaria insegna che qualsiasi eccezione di inutilizzabilità sul punto porta ad ottenere un – quasi – automatico provvedimento di rigetto).
Inoltre, dandosi per scontata la ritualità delle procedure acquisitive poste in essere dall'Autorità giudiziaria francese (in virtù del richiamato principio del mutuo affidamento), si solleva, di fatto, il Giudice nazionale dalle sue funzioni

[60] G. Giostra, Contraddittorio (principio del), in *Enc. Giur*., Roma, 1991, p. 1

[61] Conseil constitutionnel, 8 aprile 2022 n. 2022-987, M. Said Z., in *www.cortecostituzionale.it* (servizio studi Area di diritto comparato) «La questione di costituzionalità sollevata dalla Corte di cassazione atteneva a mezzi di ricerca della prova nel procedimento penale che coinvolgessero strumenti di captazione di dati informatici. In particolare, si contestava la possibilità, per il procuratore della Repubblica, in sede di inchiesta, e per il giudice istruttore, durante l'istruttoria formalizzata, di ricorrere a strumenti di captazione coperti dal segreto di Stato. L'utilizzo di tali strumenti, possibile nell'ambito di procedimenti aventi a oggetto reati di criminalità organizzata, si riteneva che ledesse le garanzie processuali, in ragione del segreto opponibile e della conseguente limitazione del contraddittorio sul punto delle tecniche di captazione utilizzata. Il Conseil constitutionnel ha sottolineato, in primo luogo, come le previsioni contestate si fondino sulla necessità di contemperare, da un lato, le esigenze di ricerca degli autori dei reati e della repressione di questi e, dall'altro, quelle di protezione della sicurezza dello Stato. In secondo luogo, si impone alle autorità procedenti di dare adeguatamente conto delle ragioni per le quali si proceda attraverso strumenti coperti da segreto. In terzo luogo, si chiarisce che nel fascicolo istruttorio tutte le informazioni ottenute vengono riversate, così come le motivazioni addotte per il ricorso allo strumento protetto, con il che l'unico elemento sottratto al contraddittorio è la tecnica di captazione coperta dal segreto di Stato. Infine, qualora ne ravvisi le condizioni, la giurisdizione può richiedere la rimozione del segreto di Stato. In ragione di queste considerazioni, il Conseil ha ritenuto che la conciliazione tra interessi confliggenti possa dirsi adeguata e che quindi le disposizioni censurate non sia lesive della Costituzione».

di valutazione e controllo sulla legittimità della prova, minando così in radice la sua imparzialità ed indipendenza funzionale[62].

Così come infatti sottolineano alcuni autori[63], il concetto di indipendenza funzionale attiene propriamente al momento di applicazione della legge e si dovrebbe tradurre nel divieto che altre diverse autorità (dunque anche quelle estere) possano comprimere tale peculiare funzione del giudice, pretendendo di dargli ordini o suggerimenti circa il modo di giudicare in concreto.

Eppure, in passato, sempre con riferimento ad altra tecnologia di comunicazioni criptate (Blackberry), la Suprema Corte di Cassazione[64] offriva la possibilità alle difese di ottenere, non solo, la versione originale e criptata dei messaggi; inoltre, anche le chiavi di sicurezza necessarie per la lettura in chiaro degli stessi («*In tema di intercettazioni di comunicazioni, ove l'attività di messa in chiaro di messaggi critpati - nella specie scambiati mediante sistema Blackberry - sia svolta dal fornitore del servizio fuori dal contraddittorio, la difesa ha diritto di ottenere la versione originale e criptata dei messaggi e le chiavi di sicurezza necessarie alla decriptazione, a pena di nullità ex art. 178, lett. c) c.p.p.*»).

Non varrebbe a comprimere il principio del contraddittorio neppure l'affermazione secondo cui: «*in tema di intercettazioni della messaggistica scambiata con i sistemi cifrati Sky Ecc […] l'utilizzo dell'algoritmo* (per la decriptazione) *esclude la possibilità di alterazioni o manipolazioni dei testi captati, in quanto, secondo la scienza informatica, ne consente la fedele riproduzione, salvo l'allegazione di specifici elementi di segno contrario*».

Invero, se da un lato appare possibile sostenere che l'algoritmo utilizzato escluda nella maniera più assoluta eventuali alterazioni del testo poiché si tratta di un'operazione *on/off*; dall'altro canto sembra altrettanto plausibile

---

[62] P. Tonini, *Manuale di procedura penale*, Milano, 2012, p. 71 «Il potere giudiziario ha la funzione di emanare sentenze, e cioè di applicare la legge al caso concreto. In base alla Costituzione il giudice è soggetto soltanto alla legge e non ad altra fonte. L'indipendenza del giudice è garantita dalla Costituzione attraverso un apposito organo, e cioè il consiglio superiore della magistratura. L'imparzialità del giudice è stabilita dal nuovo comma 2 dell'art. 111 Cost. in base al quale ogni processo si svolge davanti a un giudice terzo e imparziale. […] Non esistono controlli esterni al potere giurisdizionale per l'ovvio motivo che, altrimenti, questo non sarebbe più indipendente. […] Nel testo della Costituzione, così come modificato dalla legge n. 2 del 1999, le norme sulla giurisdizione contengono al loro interno quelle sul giusto processo: ciò ha un profondo significato. Si impone la conclusione che non può esservi giurisdizione senza giusto processo. Non è sufficiente che la Costituzione garantisca un giudice indipendente […] occorre anche che sia garantito lo svolgimento della sua funzione».

[63] V. Crisafulli – L. Paladin, *Commentario breve alla Costituzione,* Padova, 1990, p. 638.

[64] Cass. sez. IV, 15 ottobre 2019, n. 49896, in *www.dejure.it*.

ritenere che, non essendo chiare e note (perché coperte dal segreto di Stato francese) né le modalità di conservazione dei dati, né le procedure né, tantomeno, i soggetti che hanno effettuato la masterizzazione su CD-ROM dei dati trasmessi con O.I.E. ai diversi Uffici di Procura italiani, né quelli che sono entrati in contatto con tali dispositivi magnetici, esiste – quantomeno in via astratta – il pericolo che detti dati possano aver subito una manipolazione o alterazione.
È proprio l'esistenza di un "pericolo teorico" a rendere tanto più necessaria la facoltà per gli interessati di conoscere le modalità, le procedure ed i singoli passaggi che hanno portato all'estrapolazione e all'acquisizione dei dati in questione.
Non convince neppure l'affermazione secondo cui i principi di mutua fiducia e del reciproco riconoscimento non possano in alcun modo affievolire i diritti fondamentali garantiti alle persone interessate[65].
In primo luogo, perché come già accennato il momento di valutazione dell'utilizzabilità della prova estera non può che avvenire secondo le regole dettate dall'ordinamento in cui quella prova è chiamata ad esprimere il suo contenuto conoscitivo[66]; pertanto, ogni qualvolta vi è un dubbio che la prova

[65] Tra le varie: Cass., sez. VI, 27 aprile 2020, n. 12975, in *www.dejure.it*; Cass., sez. IV, 4 aprile 2023, n. 18511, in *www.dejure.it*; Cass., sez. IV, 12 aprile 2023, n. 18523, in *www.dejure.it*; Cass., sez. IV, 18 aprile 2023, n. 16347, in *www.dejure.it*; Tribunale di Reggio Calabria, Sezione per il Riesame delle misure cautelari personali, Ord. 5 novembre 2022, n. 801; Tribunale di Reggio Calabria, Sezione per il Riesame delle misure cautelari personali, Ord. 19 novembre 2022, n. 868. «Va ribadito il principio di diritto, già espresso in tema di rogatoria internazionale, secondo cui trovano applicazione, per il principio *locus regit actum* e in conformità ai canoni di diritto internazionale della prevalenza della lex loci sulla lex fori, le norme dello Stato in cui l'atto viene compiuto e non quelle del codice di rito del Paese richiedente che disciplinano il processo: la prova non può essere in contrasto con i principi inderogabili dell'ordinamento giuridico italiano e, quindi, con l'inviolabile diritto di difesa; le concrete modalità di assistenza difensiva sono regolate, per la presenza della lex loci, dalla legge dello Stato in cui viene compiuto l'atto; l'utilizzazione degli atti trasmessi dalle autorità giudiziarie straniere non è condizionata all'accertamento da parte del giudice italiano, della loro regolarità vigendo una presunzione di legittimità dell'attività svolta, spettando al giudice straniero la verifica della correttezza e l'eventuale risoluzione di ogni questione relativa alle irregolarità riscontrate con i principi inderogabili dell'ordinamento interno».
[66] F.R. Dinacci, *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, op. cit., p. 144 «La prospettiva non si pone in contrasto con l'obbligo di osservanza della lex loci stabilito dall'art. 3, comma 1, della Convenzione europea di assistenza giudiziaria. Tale obbligo, infatti, non viene violato dal momento che l'assunzione della prova all'estero viene effettuata secondo le regole di quello Stato. Ma la situazione, risulta evidente, non preclude alla giurisdizione utilizzatrice delle prove estere un giudizio sulla legalità delle forme assuntive. Del resto, tale possibilità è

straniera possa porsi in contrasto con i principi dell'ordinamento giuridico, il giudice italiano dovrebbe vanificarne il risultato conoscitivo.
Poi, per via del fatto che non essendo elaborato a livello europeo un *corpus* di garanzie "comuni", il rischio è quello di trasformare i principi in questione in una sorta di scorciatoia illiberale ispirata ad esigenze securitarie.
Non sembra un caso che una acuta parte della dottrina sottolinei come in tema di ordine di indagine europeo il livello di tutela delle garanzie difensive è tutt'altro che soddisfacente, risultando le stesse compromesse sotto diversi profili: innanzitutto, dal debole coinvolgimento della difesa derivante dalla mancata piena conoscenza degli elementi posti alla base dell'emissione dell'ordine che rimangono circoscritti ad un dialogo riservato tra le autorità giudiziarie di emissione e di esecuzione, senza margini di intervento dell'indagato; poi, dall'insussistenza di un efficace sistema di eurodifesa che consenta un tempestivo contatto e coordinamento tra difensori operanti in diversi ordinamenti, con il conseguente rischio per il difensore straniero di veder limitato il proprio diritto di assistere al compimento delle operazioni investigativo-probatorie o di accedere prontamente agli atti del processo, indebolendo così la dialettica accusa-difesa[67].
Per tali ragioni, quantomeno nella prospettiva di chi scrive, vista la (naturale) tendenza ad una sempre maggiore cooperazione giudiziaria ed interforze tra gli Stati dell'Unione europea dovuta alle nuove forme di criminalità, l'auspicio è che venga coniato quanto prima uno *ius commune* per la salvaguardia dei diritti fondamentali[68].
Solo in tal modo, infatti, si potrà, da un lato, evitare forzature sistemiche funzionali a ricercare la verità ad ogni costo; dall'altro, garantire un equo e sereno processo agli indagati-imputati.

ribadita dalla stessa rilevanza della legge del luogo, la quale non potrà che essere quella nell'ambito del quale il dato conoscitivo viene utilizzato».

[67] R. M. Geraci, *Il mutuo riconoscimento nella cooperazione processuale: genesi, sviluppo, morfologie*, in op. cit., p. 279-280.

[68] In argomento V. Manes – M. Caianello, *Introduzione al diritto penale europeo: fonti, metodi, istituti, casi*, Torino, 2020, p. 19; G. Silvestri, *Verso uno ius commune europeo dei diritti fondamentali*, in *Quad. Cost.*, 2006, p. 7 ss.